Before the
Federal Communications Commission
Washington, DC 20554

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

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President, Government Affairs

Rebecca Schwartz
Director, Regulatory and Government Affairs

Patrick Sullivan
Director, Technical and Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street, N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

Its Attorneys

January 14, 2010

TABLE OF CONTENTS

SUMMARY

The Internet is a highly dynamic and constantly evolving network of networks, and its steady growth and development is a key driver to the future of the American and global economy. Indeed, under the current U.S. regulatory regime, the broadband Internet has taken a central role in our society, advancing the ways we work, are entertained, get information and communicate. The issues involved in this proceeding strike at the heart of today's broadband world. As such, the Commission must be mindful of the Internet's history and ensure that future investment and innovation in the network are not hindered to the detriment of consumers. TIA urges the Commission to recognize the success of its current regulatory approach and not replace it with prophylactic rules. To date, the Commission's flexible approach has served the public interest and led to consumer benefits by permitting content, application and network providers to respond to customer needs and to rapid technological change.

The "open Internet" is and always has been a managed Internet. The Internet relies on a highly intelligent core and management occurs across the network on an ongoing basis. From the precursors of the Internet (ARPANET and CYCLADES) to the present, a pragmatic approach to network engineering has defined the Internet's technical evolution. Although this approach initially relied on end-to-end concepts, such reliance was practical, not dogmatic, and is too often overstated by advocates of "neutrality." There has always been intelligence at the core of the network and this intelligence has consistently been used to promote the user experience. As the network has developed since its inception, there has been a consistent move away from the "dumb pipe" conception with more and more intelligence residing in the network core through the use of many varied management techniques. If the Commission wants to preserve today's "legacy of openness and transparency" it should acknowledge and respect the Internet's development to date.

To that end, the Commission's current approach, as embodied in its 2005 *Policy Statement*, reflects the appropriate regulatory framework, ensuring that the vitality and openness of today's Internet is maintained in the future. The Commission should decline to replace this flexible framework with prophylactic rules. The *Policy Statement* has been a success, with only one case of alleged misconduct following its release. Given the lack of compelling evidence of an y widespread problem under the Commission's current regime, there is no need to tighten the regulatory environment in the name of preserving the open Internet.

If the Commission chooses to adopt rules notwithstanding the success of the current approach, it should limit itself to the four principles of the *Policy Statement* and a fifth principle of *consumer* disclosure. Policymakers should be mindful that "discrimination" is often employed to further pro-competitive, pro-consumer purposes, and should not be barred. Where network resources are overwhelmed by the rising demands on the network, network management techniques – which include certain forms of discrimination – offer consumers a path to a high-quality broadband experience. Meanwhile, TIA agrees the market will function best if the Commission adopts a consumer-based disclosure principle that calls for users to be informed of the capabilities and limitations associated with competing broadband offerings.

If the Commission elects to adopt rules, it also must be sure to frame its proposed exceptions broadly to ensure continued innovation and investment in broadband infrastructure. In particular, the Commission must adopt an expansive and flexible definition of "network management" that reflects the functionality of contemporary broadband networks. The Commission must also recognize and ensure that any new rules do not inhibit the growth of managed services or hamper the efforts of providers to respond to demands of law enforcement, public safety, and homeland security.

In addition, any rules adopted in this proceeding must acknowledge the important distinctions among different broadband platforms and the ways in which these distinctions affect network management requirements. Any approach to network management must recognize that each provider utilizes specific management tools on their network in light of their own operational situation. The Commission should ensure that it does not take any action that will significantly impact one broadband platform in favor of another.

Finally, the Commission should continue to rely on case-by-case evaluation of alleged harms rather than adopting specific enforcement rules and procedures. In the real-time environment of network management and given the highly dynamic status of broadband networks, case-by-case evaluation allows for the Commission to focus on a specific allegation of misconduct and reach a timely resolution. A case-by-case approach also permits a thoughtful, calibrated approach to network management that is responsive to the changing market and technological conditions, yet still is capable of addressing harmful conduct.

Before the
Federal Communications Commission
Washington, DC 20554

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

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

INTRODUCTION

It is well established that the Internet is a highly dynamic and constantly evolving network of networks.[1] Spurred in large part by a continuous cycle of innovation, investment and consumer demand, the Internet's steady growth and development is a key driver to the future of the American, and, indeed, the global economy. Recent advances in the broadband network have driven consumer demand for bandwidth-intensive applications such as voice over Internet Protocol ("VoIP"), audio and video streaming, video conference calling and peer-to-peer file-sharing, which has encouraged even greater demand for broadband services and resulted in a completely new trend of Internet usage patterns. It cannot be emphasized enough that under the current U.S. regulatory regime, the broadband Internet has taken a central role in our society.

As the leading trade association for the information and communications technology industry, the Telecommunications Industry Association ("TIA") shares the Commission's goal of

[1] *See, e.g.*, National Science Foundation, *The Internet changing the way we communicate*, at 11, *available at* http://www.nsf.gov/about/history/nsf0050/internet/pdf.htm.

promoting the ubiquitous deployment and adoption of broadband services.[2] TIA's 600 member companies manufacture or supply the products and services used in the provision of broadband and broadband-enabled applications. The issues involved in this proceeding are of great importance to the organization's member companies, as they impact investment in and deployment of next-generation broadband networks, applications, and devices across the United States, and ultimately the rest of the world. Just like the Commission, TIA wants to see broadband deployed everywhere and used by everyone, and the organization looks forward to continuing its partnership with the Commission in furtherance of this important objective.

In this proceeding, TIA appreciates the Commission's observation that the "Internet's openness and the transparency of its protocols have been critical to its success."[3] TIA could not agree more. TIA's members all benefit from these two pillars of the Internet's foundation. Thus, the Commission can – and should – monitor the development of the broadband market and take action where required to preserve those dual goals. However, the "open Internet" is – and always has been – a managed Internet. Indeed, as the cycle of innovation, investment and consumer demand continues, the core of the broadband network has become increasingly intelligent to better manage the staggering growth in demand for the latest broadband applications and services. Particularly in light of the lack of any demonstrated harm, TIA is concerned that any effort to develop rules under the guise of enhancing the open Internet will in fact hinder investment and innovation in a way that could seriously undermine the continued evolution of the network, all to the detriment of consumers.

[2] *See, e.g., A National Broadband Plan for Our Future*, Notice of Inquiry, 24 FCC Rcd 4342 (2009).

[3] *Preserving the Open Internet, Broadband Industry Practices*, Notice of Proposed Rulemaking, 24 FCC Rcd 13064 ¶3 (2009) ("*NPRM*").

Before it takes any action in this proceeding, the Commission must recognize that its current regulatory approach, as reflected in its *Policy Statement*,[4] has been successful in promoting a vibrant Internet ecosystem and in encouraging significant investment in the development and deployment of broadband infrastructure. The success of the Commission's approach has depended in large part not only on the willingness and authority of the Commission to police anticompetitive conduct, but on the *flexibility* the approach affords to content, application and network providers; consumers; and the Commission itself. Consequently, the Commission should decline to replace the flexible approach allowed by the *Policy Statement* with prophylactic rules.

In sum, the Commission must act with great care as it contemplates the proposals set out in the *Notice*. At the most, the Commission should consider adopting an additional principle of disclosure that is focused on the needs of consumers. In the event the Commission decides to adopt additional rules, it must ensure that there is sufficient flexibility to allow broadband Internet service providers and infrastructure manufacturers to provide managed services and to continue the use of reasonable network management tools to meet the needs of subscribers, public safety, law enforcement and homeland security. Finally, the Commission should continue to rely on a case-by-case approach to alleged violations so as to permit continued innovation in broadband services while still guarding against anticompetitive conduct.

I. THE OPEN AND TRANSPARENT INTERNET RELIES (AND ALWAYS HAS RELIED) EXTENSIVELY ON INTELLIGENCE THROUGHOUT THE NETWORK, NOT ON A MYTHIC "DUMB PIPE"

The open Internet is, and always has been, a managed Internet. It relies on a highly intelligent network core, and management occurs across the network on an ongoing basis.

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

Before the Commission looks to impose rules to "preserve an open Internet,"[5] it is highly instructive to review the evolution of the Internet structure and to understand how today's broadband network functions and how it handles consumer use and demand. It is a fundamental mistake to conceive of the Internet as a static end-to-end network and to perpetuate the myth of the "dumb pipe" as the foundation of today's open Internet. Instead, the developments described below highlight the historic role of network intelligence and management on the Internet. Needless to say, efforts to impose new network management rules may only serve to upset the current structure of the Internet ecosystem, which in turn will *undermine* the Commission's goal of "maintaining" – and building on the success of – today's open Internet.

A. The Internet's Initial End-To-End Bias Was A Pragmatic Engineering Decision, Not A Philosophical Commitment

From the Internet's earliest days, network design has focused on achieving the needs of the network's users through pragmatic engineering. The inventors of the Internet learned from earlier efforts and adapted their design to solve problems that arose as they worked. The original Internet was an amalgamation of ideas and functionalities – drawn from predecessors including ARPANET and CYCLADES – that made the most sense for the time. This pragmatic approach toward the network continues from the earliest days of the Internet to today.

One of the first network systems was ARPANET, which was a "proof-of-concept" demonstration of a packet-switched network[6] developed in the late 1960s based on ideas formulated earlier in that decade. Designed for the Defense Advanced Research Projects Agency ("DARPA") by a civil contractor, the network itself was largely a "black box" that handled all

[5] *NPRM* at ¶2.

[6] In a packet-switched network, computers communicate by dividing their messages into small packets of data that are individually routed through the network and reassembled by the recipient. No dedicated connection is established or maintained between the sender and receiver. This contrasts with a circuit-switched network (like the traditional telephone system) where the network creates and sustains a constant, dedicated connection between the communicating entities.

networking functions with minimal instruction from the end-user's hardware or applications. This "intelligence in the core" approach had advantages – for example, it simplified the creation of applications, since nearly all networking functions were handled by the network.[7] But the approach also gave rise to costs. Engineers who wanted to experiment with new networking approaches found it very difficult to modify the operation of ARPANET itself, because all of the intelligence resided in the network.[8]

One of the first internetworking systems designed for network engineering experiments was CYCLADES, a French system developed in the early 1970s that kept only the simplest networking functions in the core of the network.[9] This approach fit the needs of CYCLADES users for several reasons. First, the CYCLADES design increased efficiency by simplifying the network and pushing certain functions such as error-checking out to the edge, where they need to be performed only once per communication instead of multiple times throughout the network. Keeping the network simple also allowed data to travel over multiple, redundant paths through the network, relying on the receiver to reassemble data properly. This improved the robustness of the system. Finally, the CYCLADES network made it easier to interface with any number of other networks, creating one of the first network of networks – or "internet."

Perhaps most importantly, by installing many networking functions in the end computers, CYCLADES's designers opened up ARPANET's "black box," simplifying the development of new networking protocols. The experimental convenience of implementing the network intelligence at the edge of the network was a pragmatic solution to encourage experimentation,

---

[7] *See* Richard Bennett, Information Technology and Innovation Foundation, *Designed for Change: End-to-End Arguments, Internet Innovation, and The Net Neutrality Debate* 7-8 (Sept. 2009), *available at* http://www.itif.org/index.php?id=294 ("*Designed for Change*").

[8] *Id.* at 9.

[9] Louis Pouzim, *Presentation and Major Design Aspects of the CYCLADES Computer Network*, Third Data Communications Symposium (Nov. 1973), *available at* http://rogerdmoore.ca/PS/CYCLB.html.

not an engineering judgment that innovation always must be focused on the edge. Thus, CYCLADES enabled an iterative, evolutionary approach to improving network performance while still meeting the needs of end users.[10] But while the CYCLADES approach facilitated the development of new protocols at the network's "edge," network engineers expect to deploy any newly developed networking functions wherever it makes the most sense, including in the core of the network.[11]

The designers of the Internet relied on both the ARPANET and CYCLADES experiences when they developed the TCP/IP protocols that today form the software backbone of the Internet.[12] Like ARPANET, the Internet allowed many different models of computers to talk to each other in a common "language" using packet-based switching, which unleashed a whole new realm for innovative computer applications. Like CYCLADES, the Internet was an "internetwork" intended to connect multiple disparate networks, yet withstand failures of individual nodes.[13] Finally, the Internet facilitates both application experimentation (like ARPANET) and network experimentation (like CYCLADES).

The history described above often has been lost in debates over network management practices. In the telling of those who advocate "net neutrality" regulation, the "end-to-end"

---

[10] *See id.* ("This concern for built-in evolutionism translates itself in putting as few features as possible at levels buried in the sensitive parts of the network. With experience gradually building up, and depending on trends in international standards, more stable characteristics will eventually emerge. By putting them at some lower system level, it will be possible to obtain higher efficiency and reduce duplication, at the cost of freezing a few more parameters.").

[11] *See, e.g., Designed for Change* at 23. ("The consensus in the Internet community is that, *to the extent feasible*, end-to-end implementations . . . are preferred over network-based solutions. The discussion continues as to how we evaluate feasibility at Internet scale and what we do when endpoint implementations aren't practical.") (emphasis added).

[12] The Transport Control Protocol ("TCP") is the "smart" protocol that resides on the end-users' computers and handles congestion, error-correction and other major networking functions. The Internet Protocol ("IP") is the "dumb" protocol that handles lower-level transmissions of packets from computer to computer and is today installed in every router throughout the Internet. ARPANET eventually replaced its initial protocol with TCP/IP.

[13] Vinton G. Cerf and Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, IEEE Transactions on Communications 22(5) (May 1974), *available at* http://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf (last visited Dec. 13, 2009).

approach is cast *not* as the pragmatic engineering tool it was – designed for certain purposes but also subject to important limitations – but rather as an essential, inflexible and intrinsic feature of the network, largely (or fully) responsible for the Internet's openness and transparency.[14] In fact, it is not an inherent aspect of the Internet's structure, nor is it responsible for the network's openness.[15] To the extent the Internet favored CYCLADES's use of neutral protocols that placed more intelligence at the network's edge over ARPANET's placement of intelligence in the network's core, that outcome reflected only engineers' practical needs at the time. As described below, however, the development of the network since then, starting with the TCP/IP protocol itself, has reflected a consistent move *away* from the "dumb pipe" network, with the placement of more and more intelligence in the network's core.

B. From The Beginning, Engineers Have Managed the Rapidly Evolving Internet By Embedding Intelligence In The Network

As explained in this section, the years since the Internet's advent have been characterized by a consistent push to situate intelligence in the core of the network. The end result has been that the Internet continues to evolve and gain intelligence in a way that the initial developers could never have imagined, particularly with respect to traffic management. These developments have promoted user interests, openness and transparency and given rise to today's robust Internet ecosystem.

Since shortly after the Internet "went live," engineers have revised and modified the Internet to accommodate growing and changing traffic. Many of these approaches have directed

[14] *See, e.g., NPRM* at ¶19 ("TCP/IP reflects a so-called 'end-to-end' system design, in which the routers in the middle of the network are not optimized toward the handling of any particular application, while network endpoints (the user's computer or other communicating device) are expected to perform the functions necessary to support specific networked applications.").

[15] Indeed, one of the leading papers on the benefits of end-to-end systems notes that "the end-to-end argument is not an absolute rule, but rather a guideline that helps in application and protocol design analysis." J.H. Saltzer, *et al.*, "End-To-End Arguments in System Design." ACM Transactions on Computer Systems, Vol. 2 No. 4, 285 (Nov. 1984) ("*Saltzer et al*.").

functionality to the core of the network in order to increase efficiency as engineers have moved further and further away from a rigid end-to-end approach. These decisions have benefited consumers. After briefly summarizing the dramatic transformation of the Internet since its inception, we detail some of the approaches network engineers have used to increase intelligence in the core of the network and supplement TCP/IP in this rapidly changing environment.

1. The Internet of today differs radically from that of decades past in terms of traffic volume, traffic type, and traffic flow

It is something of an understatement to say that traffic on the Internet has changed since it was first developed. The change in volume alone has been massive. For at least the last seven years, conservative estimates indicate that Internet traffic has grown 50 percent annually.[16] In 1990, the Internet is estimated to have carried approximately one terabyte of data per month.[17] By 2008, estimates indicate that the Internet was carrying between five and nine *million* terabytes per month.[18] Thus the Internet grew by as much as 1,297 terabytes per day during that period.[19]

But not only has the Internet grown in terms of number of packets traversing the network, the type of applications sending data across the Internet has also changed. Traffic on the early Internet consisted primarily of emails and (later) web pages, with transfers of small files back and forth between the host computers. These applications are generally latency-insensitive, as

[16] University of Minnesota, *Minnesota Internet Traffic Studies*, *available at* http://www.dtc.umn.edu/mints/2002-2009/analysis-2002-2009.html (last visited Dec. 14, 2009).

[17] K. G. Coffman and A. M. Odlyzko, AT&T Labs – Research, *Growth of the Internet* (2001), *available at* http://www.dtc.umn.edu/~odlyzko/doc/oft.internet.growth.pdf.

[18] Cisco Systems, Inc., *Visual Networking Index – Introduction*, *available at* http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html#~forecast (last visited Dec. 22, 2009).

[19] By comparison, a scanned copy of every newspaper in the world published in 2003 would total approximately 139 terabytes. Peter Lyman and Hal R. Varian, *How Much Information* (2003), *available at* http://www.sims.berkeley.edu/how-much-info-2003.

receiving an email or a file with a second or two delay is largely imperceptible to the end user.[20] Today's popular applications – especially video – are placing rapidly increasing demands on the network. For example, Internet video in its various forms (streaming video on demand, Internet Protocol television ("IPTV"), and peer-to-peer ("P2P")) currently accounts for approximately 25 percent of all Internet traffic.[21] Cisco projects that Internet video will account for nearly 91 percent of all consumer IP traffic by 2013.[22] Peer-to-peer traffic has also grown wildly since the Internet's beginnings; one study estimates that P2P traffic alone accounts for 43 to 70 percent of Internet traffic in certain regions of the world.[23] This massive growth in demand not only raises traffic concerns, but also security, reliability and law enforcement issues.

Even the ways in which traffic flows on the Internet have changed. A recent study concluded that within the last five years, the core of the Internet has transformed radically, such that today the majority of Internet traffic (by volume) flows directly among large content providers, datacenter and content delivery networks, and consumer networks, rather than through Tier 1 backbone service providers.[24] This means that the majority of traffic now runs through the private networks of application providers such as Google or through content delivery networks such as Akamai that provide speedier delivery of high bandwidth content, including video. This dramatic shift in traffic flows is a significant point and dramatically underscores the role of the intelligent network in today's broadband world.

---

[20] Even so, the first version of the World Wide Web Hyper Text Transfer Protocol slowed early Internet traffic to a crawl due to side effect of an earlier congestion workaround. *See* Designed for Change at 33-34.

[21] ATLAS Internet Observatory, *2009 Annual Report*, at 28, *available at* http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf ("*ATLAS 2009 Annual Report*").

[22] Cisco, Inc., *Cisco Visual Networking Index: Forecast and Methodology, 2008-2013, available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html.

[23] *See* Ipoque, *Internet Traffic 2008/2009, available at* http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009 (last visited Dec. 14, 2009).

[24] *See ATLAS 2009 Annual Report*.

Developments such as these have placed a growing premium on network management. As explained in depth in the declarations and other materials attached to these comments, the increased use of shared network capacity (in the edge on cable and wireless networks, and in the "middle mile" and other network segments for all platforms) and growing bandwidth needs have combined to place great strains on network resources.[25] Moreover, there is no feasible way to solve these problems solely via the addition of capacity.[26] Thus, network engineers have worked to create management tools that rely on the network's intelligence to ensure that users' needs are met and that the benefits of a robust Internet continue to be enjoyed by all. These tools often necessitate use of network intelligence to identify packets as requiring certain levels of prioritization, or to otherwise classify packets, and to afford different packets the differential treatment necessary to serve consumers' needs.

2. To meet the changing needs of the Internet's users, engineers have embedded more intelligence in the network through a variety of means and in a variety of places

The open Internet is a managed Internet, preserved through an intelligent network that uses numerous tools to meet the evolving demands of consumers. Indeed, even the earliest implementations of the Internet did not require or intend for the network to treat all packets identically. This is clear from the historical design of IP packets – the electronic "envelopes" that carry information over the Internet. This design includes (and has *always* included) a service parameter that allows communicating computers to indicate to network routers that certain messages deserve precedence over other messages.[27] In other words, the IP design

[25] *See, e.g.*, Declaration of Matt Tooley and Don Bowman at 25 ("Tooley/Bowman Declaration"); Declaration of Kenneth Ko and Kevin Schneider at 4-7 ("Ko/Schneider Declaration").

[26] *See, e.g.*, Tooley/Bowman Declaration at 22.

[27] William Stallings Data and Computer Communications, 4 Ed., 513 (1994); *see also* Douglas A. Hass, *The Never-Was-Neutral Net and Why Informed End Users Can End the Net Neutrality Debates*, 22 Berkeley Technology Law Journal 1563, 1566 (2008), *available at* http://ssrn.com/abstract=957373 ("*The Never-Was-Neutral Net*").

contemplated an Internet in which certain packets could be prioritized over others. Also, while this approach was rudimentary, it certainly reflects even an early effort to enable intelligence in the network for network management purposes.

Since then, it has become apparent that more solutions were needed to complement TCP/IP networking to handle the growing traffic on the Internet. Given the radical changes in the volume, content and use of the broadband network described above, it should not be a surprise to learn that network engineers and developers continue to look beyond the end-to-end "dumb pipe" presumption by placing more capabilities within the network itself. Below, we catalog some of the techniques now in place to "manage" the Internet and preserve its useful and open nature. Then, we highlight two of the economic solutions to handling Internet traffic – the use of tiering and of Content Distribution Networks ("CDNs").

Management Techniques

The User Datagram Protocol. The development of the User Datagram Protocol ("UDP") is one early example of an update to the Internet's design that presumed intelligence in the network's core.[28] In 1986, approximately three years after ARPANET fully transitioned to TCP/IP, the Internet began to experience extreme congestion due to TCP's reaction to packet loss. Routers of that day (and today, as well) when overloaded with traffic will simply delete packets. Unlike TCP, UDP was a "dumb" protocol that included no mechanism to handle congestion, but instead relied on the intelligence of the network to manage any resulting congestion. The development of UDP was motivated by the needs of real-time applications such as VoIP, which function better when lost packets are simply dropped than when they are resent.[29]

[28] *See generally* J. Postel, The Internet and Engineering Task Force, *User Diagram Protocol*, RFC 768 (1980), *available at* http://tools.ietf.org/html/rfc768.

[29] Richard Bennett, *Change is Part of the Internet's Design* (Oct. 2, 2009), *available at* http://www.internetevolution.com/author.asp?section_id=783&doc_id=182555 (last visited Dec. 22, 2009).

TCP is not well suited to such applications, because its built-in error-checking mechanisms impose significant delay and, in fact, exacerbate congestion by resending packets. In contrast, UDP assumes that error checking and correction is either unnecessary or is handled by elsewhere, and makes no attempt to detect or compensate for congestion. Packets sent using UDP may arrive out of order, duplicated, or not at all – depending on the operation of the network. Thus, UDP relies on intelligence in the network core for decisions as to how to address congestion. Today, a number of network applications use UDP, including streaming media applications such as IPTV, Domain Name Systems lookups, many online games and VoIP.

Routers and Jacobson's Algorithm. Another early attempt to improve the TCP/IP architecture provides an example of the complications that can arise when network intelligence is placed solely at the edge of the network. As noted above, as the early Internet developed, congestion grew, and would be exacerbated by TCP's practice of re-sending lost packets, resulting in a vicious cycle: a congested router would drop a packet, TCP would resend the packet, and congestion would consequently worsen. Two proposed fixes emerged. One, the Jain proposal, would have made the network smarter by modifying the IP to allow routers to send a message back to hosts announcing that they were congested.[30] The other, Jacobson's Algorithm, would have modified TCP to guess when congestion might be occurring, and thus delay the re-sending of packets. Because Jacobson's Algorithm did not require modifying the few hundred routers that, in 1986, made up the network, it was the chosen solution.

[30] The Jain proposal was eventually made an Internet Standard, but due to legacy routers, has not been fully deployed even today. K. K. Ramakrishnan, Sally Floyd, and David L. Black, The Internet Engineering Task Force, *The Addition of Explicit Congestion Notification (ECN) to IP*, RFC 3168 (Jan. 6, 1984), *available at* tools.ietf.org/html/rfc3168.

Jacobson's Algorithm worked, but network congestion at the edge has caused much difficulty for networks ever since.[31]

> TCP congestion avoidance mechanisms . . . are not sufficient to provide good service in all circumstances. Basically, there is a limit to how much control can be accomplished from the edges of the network. Some mechanisms are needed in the routers to complement the endpoint congestion avoidance mechanisms.[32]

Since the late 1990's, Internet network access providers and router companies have had the ability to identify and prioritize particular types of traffic.[33] These techniques have expanded continually, and newer routers can identify individual applications, traffic flows, and subscribers.[34] Today, prioritization techniques have become quite advanced, and may be configured in many different ways to ensure that jitter- and latency-sensitive traffic is delivered on a timely basis without any perceptible effect on best efforts Internet traffic.[35] In short, the ability to identify and potentially "discriminate" among packets is not a new development. One particular type of smart routing known as Multiprotocol Label Switching ("MPLS") has been the subject of the Internet Engineering Task Force standards working group since 1997.[36]

Network Security and Public Safety. Network intelligence is not, of course, only used to manage peak traffic levels. Throughout the history of the Internet, network engineers have employed various aggressive strategies such as packet blocking, dropping, and re-routing in

---

[31] Indeed, it appears that the Jacobson Algorithm and TCP flow control in general was responsible for the incredibly poor performance of the early Web. *Designed for Change* at 33.

[32] Bob Braden et al., Internet Engineering Task Force, *Recommendations on Queue Management and Congestion Avoidance in the Internet*, RFC 2309 (Apr. 1998), *available at* http://tools.ietf.org/html/rfc2309.

[33] *The Never-Was Neutral Net* at 20-21.

[34] Cisco Systems, Inc., *Creating New Broadband Tiers of Service Using Cisco Service Control Technology* (2008), *available at* http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_brochure0900aecd8024525f.html (last visited Dec. 22, 2009).

[35] *See generally* Ko/Schneider Declaration at 12-15 (describing different prioritization techniques, including use of strict priority, "round robin" approaches, and weighed algorithms).

[36] The MPLS Resource Center, *The MPLS FAQ*, *available at* http://www.mplsrc.com/faq1.shtml#MPLS%20History (last visited Dec. 22, 2009).

order to prevent or alleviate harm from hackers and other security risks.[37] Providers have also modified their networks to ensure that their operations are compatible with the needs of law enforcement, public safety, and national/homeland security. It is safe to say that the vast majority of customers and citizens expect this type of network management and would be dismayed if the Commission were to take any steps that limited the ability of service providers to manage these issues on a going forward basis.

Economic Solutions

Tiering. Tiering in this context refers to the relationship between Internet service providers, content providers and data transport providers, which can include different levels and qualities of Internet service, typically for varying prices. Tiering has been present ever since the commercial foundations of the Internet, as these providers negotiate deals to connect to each others' networks.[38] "Broadly defined, 'tiered access' refers to discrimination by a provider based on any criteria, including the price paid, the speed of the service requested, the geographical location of the service, or the nature of the traffic transmitted and received."[39] Although tiering is primarily an economic solution to congestion, many Quality of Service ("QoS") terms are dependant on the functionality of intelligent networks that is enabled by the tiering approach.

Tiering necessarily relies on an intelligent network – specifically, it often requires that the network be capable of marking packets and affording differential treatment to different packets. That differential treatment itself can take many forms. For example, networks rely on "traffic policers," which limit the rates at which different types of traffic may enter a particular network

[37] *See* Ko/Schneider Declaration at 17-18; Tooley/Bowman Declaration at 20, 22.

[38] *The Never-Was Neutral Net* at 9.

[39] *Id.* at 15. Different types of applications require different types of treatment by the network. *See, e.g.*, Tooley/Bowman Declaration at 19-20; Ko/Schneider Declaration at 9-10.

(or prevent entry entirely),[40] or "traffic shapers," which queue traffic for future delivery,[41] or prioritization of the sort discussed above.[42] These approaches only work – and only create consumer value – because today's Internet has evolved a long way from the "dumb pipe" cited by "neutrality" proponents.

Content Delivery Networks ("CDNs"). An increasingly popular approach to improving the performance of bandwidth intensive applications, such as streaming video, is the use of CDNs. CDNs can deliver extremely fast service by providing specialized servers and networks with connections at key points in the Internet infrastructure. Content providers pay CDNs to cache their content on the CDN's servers, so that when a user wishes to view particular content, that content is delivered at an improved speed. This can dramatically improve download times and streaming performance. Some of the largest content providers on the Internet, such as Google, have built their own private CDNs in order to get their content to consumers quickly and minimize potential network congestion.[43]

3. Wireless Networks Have Traditionally Been Centrally Managed, with Intelligence in Both the Core and the Handset Under Network Control

Wireless mobile data networks are not simply extensions of the Internet; their origins are vastly different from those of the Internet. In contrast to the Internet's predecessors, ARPANET and CYCLADES, the predecessors to today's wireless mobile data networks did not employ an end-to-end design paradigm. The cellular voice networks and paging networks from which today's wireless mobile data networks evolved have always been centrally controlled networks

[40] *See, e.g.*, Ko/Schneider Declaration at 13; Tooley/Bowman Declaration at 19.

[41] *See* Ko/Schneider Declaration at 13.

[42] *See, e.g.*, Ko/Schneider Declaration at 13-14; Tooley/Bowman Declaration at 19.

[43] *ATLAS 2009 Annual Report* at 18.

that employ intelligence both inside the network core and in terminal devices that effectively form part of the network itself, under network control.

Much of the computing power (and battery capacity) in user handsets has traditionally been devoted to establishing and managing the radio link. Until recently, the limited amount of computing power available for user data processing in the handset, coupled with display limitations and restricted data rates, spurred the development of solutions that relied principally on data processing in the network itself, or in other intelligent networks. A variety of network-based solutions arose over time — such as the BlackBerry device, which was originally a two-way pager used for accessing email from a centralized server;[44] and network operators' simplified "mobile web" sites that provided access to information by handsets not capable of processing and displaying websites.[45]

Central management of the radio frequency environment remains necessary even today. In the data-centric 3G and 4G world, handsets continue to be integral parts of the intelligent network, operating under central network control for purposes of establishing and maintaining the bidirectional radio link between the handset and the cellsite. Equally important, the network needs to take into account the radio conditions affecting each handset when it allocates timeslots and bandwidth to the handsets seeking to communicate through it.[46] Because of the need to manage radio transmission conditions, the handset is not outside the "edge" of the network, but is an integrated part of the intelligent network itself.

* * *

[44] *See* Ronen Halevy, The History of RIM and the BlackBerry Smartphone, Part I: The Origins (Feb. 12. 2009), *available at* http://www.berryreview.com/2009/02/12/the-history-of-rim-the-blackberry-smartphone-part-1-the-origins/.

[45] *See* Claire Woffenden, *Will Wap's Call Go Unanswered?* (June 2, 2000), *available at* http://www.computing.co.uk/vnunet/analysis/2131787/wap-call-unanswered.

[46] *See, e.g.*, Nokia Siemens Networks, *Quality of Service Solutions in HSPA RANs*, at 12 (2009), *available at* http://www.nokiasiemensnetworks.com/sites/default/files/QoS_Radio_WP.pdf ("*Quality of Service Solutions*").

As the discussion above makes clear, there has always been intelligence at the core of the Internet, and this intelligence has consistently been used to promote the user experience. If the Commission truly wants to preserve today's Internet because it "embodies a legacy of openness and transparency that has been critical to the network's success as an engine for creativity, innovation, and economic growth,"[47] it should acknowledge and respect the Internet's development to date – and specifically the dynamic, customer-focused management that has been and continues to be used every minute of every day to ensure a satisfying user experience. Those who urge a flattened view of an "end-to-end" Internet comprised of "dumb pipes" misunderstand both the Internet's history and its current structure. In evaluating the proposed rules, the Commission should be clear about what the Internet is, and *why* it is what it is. Proposals based on fundamental misunderstandings, of these two issues would only serve to disrupt an approach that has worked extremely well to date.

II. THE POLICY STATEMENT HAS SUCCESSFULLY ENABLED BROADBAND GROWTH AND SHOULD NOT BE REPLACED WITH AGGRESSIVE AND INTRUSIVE REGULATION

Like the Commission, TIA supports policies that will enhance broadband infrastructure deployment, promote facilities-based broadband competition, encourage the proliferation of broadband-enabled devices, protect against anticompetitive behavior in the marketplace, and promote consumer satisfaction. In the current regulatory environment, and notwithstanding difficult economic times, our members continue to innovate and provide the materials for investment in the broadband network to meet these important goals. Indeed, the ICT sector has seen steady growth in investment since 2003 – with 2008 investment levels of $455 billion or 22

[47] *NPRM* at ¶17.

percent of the country's capital investment.[48] Sixty-five billion dollars was invested by communications services providers in 2008 alone.[49] Given this track record of investment by the broadband industry, the Commission should be very reluctant to initiate any changes that upset its existing regulatory approach.

In the instant proceeding, the broadband ecosystem would best be served by a Commission approach to network management that reflects the successful *Policy Statement* and adds a consumer-based disclosure principle. As explained in greater detail below, there is no demonstrated need for any further action at this time. Given the lack of harm, the Commission should continue to embrace the *Policy Statement* and the flexibility it affords broadband service providers and infrastructure manufacturers. Nevertheless, in the event the Commission adopts network management rules, it should ensure that (1) its exceptions – in particular the scope of reasonable network management, the important role of managed and specialized services, and the need to serve the requirements of law enforcement, public safety and homeland security – are sufficiently flexible to allow companies to continue to invest and innovate in the network; (2) any rules accommodate differences in network platforms and do not disproportionately impact a particular technology; and (3) it employs case-by-case enforcement that is narrowly tailored to cure any anticompetitive practice found inconsistent with the Commission's rules.

The Commission should remain mindful of the successful growth of the broadband Internet under its existing regulatory structure. For example, in 2000, only 46 percent of households had access to high-speed Internet provided by a cable operator. Ten years later, that figure has doubled as cable operators now offer high-speed Internet service to more than 92

[48] *See* Bret Swanson, *Preparing to Pounce: D.C. angles for another industry*, The Technology Liberation Front (Oct. 19, 2009), *available at* http://techliberation.com/2009/10/19/preparing-to-pounce-d-c-angles-for-another-industry/ (last visited Dec. 21, 2009) (sourced from U.S. Bureau of Economic Analysis).

[49] *See id.*

percent of American households.[50] In addition, by some estimates, cumulative capital expenditures by broadband providers from 2000-2008 were over half a trillion dollars, and, as a result of this massive private investment in infrastructure, over "90% of U.S. households can choose from either a wireline or a cable broadband service and approximately four-fifths of U.S. households have access to both."[51] Finally, the biggest growth opportunity for broadband may well be mobile wireless, where estimates place productivity gains from wireless broadband services at almost $860 billion between 2005 and 2016.[52] Moreover, the U.S. already ranks first in the world with respect to wireless web access, accounting for 29.3 percent of all mobile web surfing worldwide.[53]

Not surprisingly, consumers are favorably responding to the ongoing network innovation and investment by providers and manufacturers. Consumer demand is driving a dramatic increase in broadband Internet access service adoption from less than five percent of American households in 2000, to approximately 30 percent in 2005 and 63 percent in 2009.[54] TIA estimates that there will be 79.4 million subscribers of high-speed Internet service in 2009, and, expects that figure to grow to 103 million in 2012.[55]

---

[50] *See* Comments of the National Cable and Telecommunications Association, GN Dkt No. 09-51, at ii (filed June 8, 2009).

[51] Comments of the United States Telecom Association, GN Dkt No. 09-51, at i (filed June 8, 2009).

[52] *See* Comments of CTIA-The Wireless Association®, GN Dkt No. 09-157 *et al*., at 11 (filed Sept. 30, 2009).

[53] *See id*. at 66 (citing Sarah Keefe, *U.S. tops worldwide charts for mobile web browsing and spending*, Bango (Mar. 12, 2009), *available at* http://news.bango.com/2009/03/12/us-tops-mobile-web-browsing-and-spending-charts/ (last visited Dec. 21, 2009)).

[54] *NPRM* at ¶48. *See also* John B. Horrigan, *Home Broadband Adoption 2009*, Pew Internet and American Life Project, at 11 (June 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Home-Broadband-Adoption-2009.pdf ("*Horrigan*")

[55] TIA's 2009 ICT Market Review & Forecast, Figure I-1.9 "Broadband Subscribers in the United States," ("TIA 2009 ICT Market Review & Forecast") available *at* http://www.tiaonline.org/business/research/mrf/.

A. The Commission Should Be Extremely Cautious With Regard To The Scope Of Any New Rules

The Commission's *Policy Statement* has been a positive force in technology policy.[56] Indeed, as the Commission will remember, TIA and its fellow members of the High Tech Broadband Coalition ("HTBC") proposed very similar principles almost two years before the statement was adopted. In a September 2003 letter and several subsequent filings, the HTBC urged the adoption of four "connectivity principles."[57] The *Policy Statement* adopted most (though, as discussed below, not all) of the principles set forth by HTBC. Since then, TIA has continued to support the *Policy Statement* and maintained its view that the broadband marketplace can be vigilantly monitored and complaints of anticompetitive activity can be addressed through appropriate legal and regulatory oversight offered by the *Policy Statement*.[58] Notwithstanding its ongoing endorsement, TIA is deeply concerned about the Commission's current effort to convert the *Policy Statement* into rules, particularly if that would include codifying proposed principles on non-discrimination and transparency.[59]

---

[56] *See, e.g.*, Comments of Telecommunications Industry Association, WC Dkt No. 07-52 (filed June 13, 2007) (filed in response to *Broadband Market Practices*, Notice of Inquiry, 22 FCC Rcd 7894 (2007) ("*TIA NOI Comments*").

[57] High Tech Broadband Coalition Letter to Michael K. Powell, Chairman, Federal Communications Commission, September 25, 2003, CS Dkt No. 02-52 et al. ("*HTBC September 2003 Letter*"). *See also* HTBC filings in CS Dkt No. 02-52; GN Dkt No. 00-185; CC Dkt Nos. 02-33, 95-20 & 98-10.

[58] *See TIA NOI Comments* at 11 ("TIA believes that the broadband marketplace can be vigilantly monitored and complaints of anticompetitive activity can be addressed through appropriate legal and regulatory oversight. TIA has maintained that the Federal Communications Commission (FCC) has such authority today. However, as no significant evidence of a problem exists at this time, it is not now necessary to impose any Net Neutrality-like regulations. Rather, such oversight should address any problems on a case-by-case basis in the event they arise, using the Commission's Policy Statement as guidance.").

[59] As discussed in Section II.A.2 below, TIA supports a consumer-based disclosure principle, but does not support the overly broad transparency principle proposed by the Commission in the *NPRM*.

1. The *Policy Statement* approach has been a success, with only one case of alleged misconduct following the statement's release

In suggesting that the *Policy Statement* cannot protect consumers and that rules are required to preserve the openness of the Internet, the Commission seems to find a problem where the record suggests otherwise. Although the Commission seems to draw negative conclusions about the current state of Internet openness,[60] the underlying facts paint a far different picture: first, the industry has extensively deployed broadband since the adoption of the Policy Statement;[61] and second, in the ten years of broadband Internet access, the Commission only identified two occurrences of provider conduct that necessitated enforcement action.[62] In the first case, the Commission quickly and efficiently resolved a situation in which Madison River Communications had been blocking its subscribers' ability to use certain VoIP services.[63] The only other case of alleged misconduct handled by the Commission since the adoption of the *Policy Statement* remains pending before the U.S. Court of Appeals for the D.C. Circuit.[64] There simply is no basis to reverse the FCC's prior conclusion that the policy statement provides sufficient protection to foster an open and competitive Internet.[65]

---

[60] "[B]roadband Internet access service providers may have both the incentive and the means to discriminate in favor of or against certain Internet traffic and to alter the operation of their networks in ways that negatively affect consumers, as well as innovators trying to develop Internet-based content, applications, and services." *NPRM* at ¶8.

[61] *See* discussion, *supra*, for additional details on broadband deployment in this decade.

[62] "We have in the past found evidence of service providers concealing information that consumers would consider relevant in choosing a service provider or a particular service option. For example, in *Madison River* and *Comcast*, broadband Internet access service providers blocked specific applications desired by users without informing them." *NPRM* at ¶123. The Commission also cites a study that suggests wide-spread blocking of BitTorrent protocols. *Id.* It is worth noting that only one of these two cases occurred after the release of the 2005 *Policy Statement*.

[63] *Madison River Communications*, LLC, Order, 20 FCC Rcd 4295 (EB 2005) ("*Madison River Order*").

[64] *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, Broadband Industry Practices, Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management,"* Memorandum Opinion and Order, 23 FCC Rcd 13028 (2008) (*"Comcast Order*") and Comcast v. FCC, No. 08-1291 (D.C. Cir. filed Sept. 4, 2008).

[65] *See, e.g., Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156, 168 (1962) ("The agency must make findings that support its decision, and those findings must be supported by substantial evidence."); *Eagle Broad. Group, Ltd. v. FCC*, 563 F.3d 543, 551 (D.C. Cir. 2009) (noting the applicability of the substantial evidence

The benefits arising from the *Policy Statement* stem from its flexibility and the signals it sends to market actors, rather from any prescriptive, heavy-handed requirements. Put differently, the *Policy Statement*'s lack of detailed lists of mandates and prohibitions is not a sign of its weakness, but rather a critical component of its strength. Industry and consumers have responded favorably with unprecedented levels of investment, innovation and consumer demand. For these reasons, the prophylactic regulations suggested by the Commission in *NPRM* could in fact be *harmful* to the public interest as they would disrupt the current and highly successful dynamic regime.

During the past four years, the flexibility afforded by the *Policy Statement* has not resulted in an onslaught of alleged violations but instead has facilitated breakneck network deployment and innovation – developments that have inarguably benefited consumers. The Commission itself rightly noted in the *NPRM* that since "the adoption of the *Internet Policy Statement* in 2005, alternative platforms for accessing the Internet have flourished, unleashing tremendous innovation and investment. In particular, wireless broadband Internet access has emerged as a technology that, from a consumer's perspective, now supports many of the same functions as DSL and cable modem service."[66] Given the lack of any real compelling evidence of misconduct under the Commission's current regulatory regime, there is little need to tighten the regulatory environment in the name of preserving the open Internet.

---

standard to agency factfinding); *Illinois Pub. Telecomms. Ass'n v. FCC*, 117 F.3d 555, 563-64 (D.C. Cir. 1997) (holding that the FCC acted arbitrarily and capriciously in adopting a rule unsupported by the evidence and without acknowledging contradictory evidence).

[66] *NPRM* at ¶155.

2. To the extent the Commission adopts rules, it should limit itself to the four principles of the *Policy Statement* and a fifth principle of consumer disclosure

Given the benefits consumers have enjoyed since the *Policy Statement* was adopted, the Commission should decline to modify its current approach to network management practices by broadband Internet access providers. In particular, rules permitting and/or prohibiting specific conduct, particularly with respect to discrimination, could have the perverse effect of locking in current network management assumptions, and would likely diminish consumer welfare. Finally, while TIA supports a transparency principle, such a principle must be carefully tailored to focus on consumer-based disclosure requirements.

a. "Discrimination" may be employed to effectuate pro-competitive, pro-consumer purposes, and should not be barred

The *Policy Statement*'s flexible approach to network management has played a central role in enhancing the online experience of consumers, particularly in light of the increasing demand for bandwidth-intensive services and applications that are far less tolerant of "latency" and "jitter."[67] By managing traffic in accordance with the *Policy Statement*, Internet access providers can ensure that jitter- and latency-sensitive traffic, as well as traffic designed to enhance homeland security, is assured passage through the network in a manner consistent with user needs and expectations.

But the rise of jitter- and latency-sensitive applications has produced, in turn, a challenge for network providers. Most Internet traffic is delivered on a "best effort" basis, where best effort refers to basic connectivity with no guarantees regarding delivery of every packet, and packets generally are delivered on a first-come, first-served basis. When network resources are

[67] Generally, "latency" refers to the amount of time it takes a packetized communication to traverse the network, and "jitter" refers to a phenomenon whereby the degree of latency changes during the course of a communication, such that packets arrive out of (chronological) order. *See* Ko/Schneider Declaration at 5; Tooley/Bowman Declaration at 16.

overwhelmed, the TCP/IP protocol calls for packets to be dropped and then for packets to be resent from the point of origination, further adding to congestion.[68] Modern network management techniques, which may include certain forms of discrimination, offer consumers a path to a high-quality broadband experience in light of rising demands on the network.[69] Such techniques are critical because, even under ideal circumstances, delivery of packets over the best-effort Internet without network management tools will often entail degrees of latency and jitter that are incompatible with the needs of contemporary users.[70] This is all the more important in the case of wireless data communications, because users contending for bandwidth at a given cellsite are subject to widely differing radio transmission conditions; network operators need to manage the resources allotted to users so that poor connections do not use up excessive bandwidth and thereby penalize other users with higher quality connections.[71]

Network operators can respond to these increased network needs in either of two ways. First, service providers could simply construct more and more capacity. Needless to say, thanks to the FCC's forward-looking broadband policy choices, network providers *are* adding more capacity on all manner of platforms, and TIA supports these efforts.[72] However, increased network usage cannot economically or technically be addressed through increased network

---

[68] *See*, *supra*, Section I.B.2.

[69] *See* Ko/Schneider Declaration at 12-16; Tooley/Bowman Declaration at 20-21.

[70] *See* Ko/Schneider Declaration at 9-10; Tooley/Bowman Declaration at 16-18.

[71] The scheduling algorithm used in most 3G and 4G networks for allocating time slots and bandwidth among users based on radio conditions is known as "proportionally fair" scheduling, and it has been the subject of extensive research over the years. *See, e.g.*, *Quality of Service Solutions* at 12; Tian Bu, Li Li, Ramachandran Ramjee, *Generalized Proportional Fair Scheduling in Third Generation Wireless Data Networks*, INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings 1-12 (April 2006), *available at* http://research.microsoft.com/en-us/um/people/ramjee/papers/gpf.pdf; Kuenyoung Kim, Hoon Kim, Youngnam Han, *A Proportionally Fair Scheduling Algorithm with QoS and Priority in 1xEV-DO*, 5 The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2239-2243 (Sept. 2002), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.4502&rep=rep1&type=pdf.

[72] *See, e.g.*, Robert C. Atkinson & Ivy E. Schultz, *Broadband in America: Where It Is and Where It Is Going (According to Broadband Service Providers)*, at 41, fig. 10, Major Broadband Deployments: Performance Against Announced Completion Dates (2009).

deployment alone. The deployment necessary to meet current network needs in the absence of management tools would be exorbitantly expensive, and the associated costs would fall on end users, making broadband usage uneconomic for many.[73] Moreover, network operators are unlikely to make significant additional investments without an expectation of sufficient revenues to cover the cost of deployment and a reasonable return on investment. In the case of wireless services, increasing network capacity typically requires access to additional spectrum, but the allocation and assignment of spectrum is a slow and complicated process.[74] Even on cable and wireline networks, there are technical barriers to reliance on additional capacity: no rational expansion of capacity could accommodate the traffic spikes that occur during events of great public interest (such as the recent death of Michael Jackson), or the fluid needs of a family whose members make simultaneous use of multiple distinct services (e.g., P2P downloads, high-definition video screening, and telephone service) flowing over the same facility.[75]

Second, service providers can (and indeed must) use network management techniques to ensure a quality customer experience. Reasonable network management techniques, which often require some type of pro-consumer discrimination, offer consumers a path to a quality broadband experience without the prohibitive costs of simply deploying additional capacity. Such management can ensure that jitter-and latency-sensitive traffic, as well as traffic designed to enhance public health and safety, is afforded end-to-end prioritization. Generally, traffic subject to this type of QoS management will be prioritized over other traffic, and will be protected against the packet loss that might otherwise occur when the network is taxed beyond its

[73] *See, e.g.*,Tooley/Bowman Declaration at 4, 16-18. *See also Horrigan* at 40 (detailing that a plurality of dial-up users cite price as the reason for declining to switch to broadband service).

[74] *See* Reply Comments of CTIA-The Wireless Association®, GN Dkt Nos. 09-157, 09-51,at 10-11 (filed Nov. 9, 2009) (detailing the 10 year process for licensing 700 MHz spectrum for commercial wireless use).

[75] *See, e.g.*, Tooley/Bowman Declaration at 16-18, 22-23; Ko/Schneider Declaration at 21-23.

capacity.[76] A codified non-discrimination rule could prohibit broadband service providers from taking such action in the future. At the very least, such a rule would create sustained uncertainty, thus dampening investment incentives and innovation.

In the case of wireless data, both 3G and 4G networks have QoS management built into the standards.[77] By using QoS management, traffic that is sensitive to jitter or packet loss or latency, such as VoIP, can be given appropriate resources, while spreading less-sensitive traffic over time; by such an approach, it is possible to accommodate more traffic overall while increasing the perceived quality of sensitive traffic.[78] Under the LTE standards, the network manages QoS even for non-QoS-aware applications, taking into account factors such as whether guaranteed bandwidth is necessary (and, if so, how much), the maximum bandwidth for the data stream, the user's aggregate bandwidth budget, and the data stream's tolerance for packet loss and delay.[79] This allows, for example, the establishment of high bandwidth limits for a user's business-related VPN traffic, while placing lower bandwidth limits on the user's web browsing.[80]

QoS management has become an increasingly important tool for all network providers, enabling them to ensure timely passage of time-sensitive content and applications, such as VoIP

[76] *See* Ko/Schneider Declaration at 21; Tooley/Bowman Declaration at 25.

[77] Hannes Ekström, *QoS Control in the 3GPP Evolved Packet System*, 47 IEEE Communications Magazine, Issue 2 at 76-83 (Feb. 2009), *available at* http://archive.ericsson.net/service/internet/picov/get?DocNo=5/287%2001-FGB%20101%20256&Lang=EN&HighestFree=Y ("Ekström Paper"); *Quality of Service Solutions* at 7-9.

[78] *Quality of Service Solutions* at 8 ("With the use of differentiated treatment, one can improve the efficiency of the system and avoid overdimensioning the network. . . . When no service differentiation is applied, all the traffic is treated in a similar manner. This means that in order to keep all users happy, all traffic needs to be treated in line with the most delay sensitive traffic such as VoIP. This limits the amount of users that can be served . .. . since the 'peaks' of the traffic reach the limit of the available cell throughput. When QoS differentiation is used, . . . the low priority data [] traffic is spread out over time, utilizing the 'gaps' of the other data transmission and this creates room for a new high priority VoIP user. This way, the cell throughput is enhanced by QoS differentiation at the cost of longer delays of delay insensitive traffic.").

[79] *Ekström Paper* at 77-80.

[80] *See id.* at 79.

traffic, streaming video, and telemedicine, not amenable to latency or jitter.[81] While it is true that prioritization of a traffic stream could have the effect of "discriminating against" another traffic stream, any harm from the practice is hardly a given. Prioritization's potential impact on non-prioritized traffic is the result of a number of factors, such as bandwidth availability, network engineering and traffic congestion.

In fact, prioritization can be engineered in such a manner as to have absolutely no discernible impact on non-prioritized traffic.[82] Where "deprioritization" of traffic that is not time-sensitive does occur, such delays typically last mere milliseconds – often less – and the benefits of the prioritization itself outweigh the costs imposed. That is, such management shifts resources in a way that trivially inconveniences few but provides substantial benefit to many.[83]

Notwithstanding the clear benefit and value to consumers of these sophisticated network management techniques, any Commission effort to ban all forms of discrimination-based network management could threaten the ability of service providers and infrastructure manufacturers to react on a real-time basis to constantly changing and evolving network conditions. While the Commission does contemplate "exceptions" to its rules, even the suggestion of limits ultimately will cause providers to think twice before acting during a period of congestion, which ultimately could lead to a degraded experience for customers.

(i) At the very least, any anti-discrimination rule must be limited to anticompetitive discrimination

In the event the Commission opts to impose a non-discrimination rule (notwithstanding the deleterious effects such a rule would have for investment, innovation, and consumer demand

[81] *See* Ko/Schneider Declaration at 19-20; Tooley/Bowman Declaration at 16-18. *See also* Ekström Paper at 77-80.

[82] *See* Ko/Schneider Declaration at 14 (discussing use of weighted algorithms designed to effectively eliminate any perceptible effect on best-efforts traffic).

[83] *See, e.g., Quality of Service Solutions* at 8-9

in the broadband marketplace), it must at least cabin the rule such that it proscribes only *anticompetitive* discrimination. From the inception of the American common-carriage regime, Congress and the courts have recognized that *some* discrimination will always be permissible and thus should remain lawful – and that the class of permitted behavior is not susceptible to definition via bright-line rules. Thus, the Interstate Commerce Act of 1887[84] provided (among other things) that it "shall be unlawful for any common carrier subject to the provisions of this act to make or give any *undue or unreasonable* preference or advantage to any particular person, company, firm, corporation, or locality . . . ."[85] This concept, of course, was replicated in the Communications Act of 1934, which proscribes "any *unjust or unreasonable* discrimination in charges, practices, classifications, regulations, facilities or services."[86] As the courts have recognized, these modifiers have concrete analytical force, and "discrimination" that is not "unjust or unreasonable" will stand.[87]

As currently drafted, however, the proposed nondiscrimination rule contemplated here would make no allowance for "discrimination" that benefits the public – a class of "discrimination" that, as discussed throughout these comments, is likely very large. To that end, TIA recommends that the Commission at the very least qualify the nondiscrimination rule to prohibit only "anticompetitive" discrimination. This qualifier would recognize the importance of differentiating among traffic types, and would give providers latitude to pursue steps that maximize consumer benefit.[88]

---

[84] Interstate Commerce Act of 1887, 49 Cong. Ch. 104, 24 Stat. 379 (1887).

[85] *Id.* § 2 (emphasis added).

[86] 47 U.S.C. § 202(a) (emphasis added).

[87] *See, e.g.*, *Orloff v. FCC*, 352 F.3d 415 (D.C. Cir. 2003).

[88] TIA notes that the bar on "anticompetitive" discrimination would permit some activity that might be prohibited by a bar on "unreasonable" discrimination. This distinction is appropriate because, unlike the rail services contemplated by the ICC or the legacy communications networks contemplated by the Communications Act of

b. TIA and its members support customer disclosure, but the Commission's proposed transparency principle is far too broad and potentially too burdensome

Although it would be imprudent for the Commission to adopt rules governing network-management and transparency as currently proposed, TIA agrees the market will function best if the Commission adopts a *consumer*-based disclosure principle that calls for users to be informed of the capabilities and limitations associated with competing broadband offerings. Such information will enhance the operation and efficiency of the market, ensuring that economic signals reflect consumers' actual knowledge rather than their assumptions. It also will minimize the confusion and anger that arises when customers discover limitations that providers had not previously or adequately disclosed. A consumer disclosure principle can be an essential component of the Commission's desire to preserve the vibrancy of the broadband market.

It is axiomatic that free markets require the free flow of information regarding the goods and services for sale. Indeed, economists often cite a lack of information as one of the two main causes of market failure.[89] This principle applies to the broadband market as well. For this reason, TIA has long urged the Commission to adopt a principle that calls for consumers to receive relevant information regarding their broadband service plans.[90] Consumers must have meaningful information regarding aspects of their plan, including upstream and downstream throughput speeds, bandwidth usage limitations, the use of technologies designed to block spam, viruses, or other content deemed to be harmful, and any other limitations associated with a

---

1934, the broadband Internet access market at issue here is competitive, and the market itself can regulate against unreasonable practices. At the most, therefore, the rule should proscribe only "anticompetitive" conduct – *i.e.*, conduct that calls into question the market's very ability to police provider behavior.

[89] *See, e.g.*, Robert S. Pindyck & Daniel L. Rubinfeld, Microeconomics 294 (5th ed. 2001) ("Market failure can also occur when consumers lack information about the quality or nature of a product and so cannot make utility-maximizing purchase decisions. Government intervention (e.g., requiring 'truth-in-labeling') may then be desirable."). The other principal cause for market failure is the presence of externalities. *Id.*

[90] *See HTBC September 2003 Letter*.

particular service plan.[91] The provision of such meaningful information regarding broadband service plans will allow consumers to make informed decisions among competing providers and will enable the Commission to rely on the market in the first instance, rather than on heavy-handed regulation, to address claims of misconduct.[92]

While TIA supports a new principle of *consumer* disclosure, it cannot support the Commission's proposal to codify an overly broad sixth principle regarding transparency. First and foremost, TIA is concerned with the Commission's proposal to police the availability of information about the traffic management practices of networks to "content, application, and service providers as well as the government."[93] Broadband service providers should not be forced to disclose potentially sensitive network management information for the purpose of "benefit[ing] content, application, and service providers and investors."[94] The Commission appears to have its priorities reversed in this situation. Absent a clear track record of harm, it is unclear why the Commission would potentially upset the management of the broadband network by requiring broadband Internet access providers to ensure that content and application providers have detailed information about network management practices.[95] Given the existing challenges of managing an increasingly sophisticated network, this seems like a questionable undertaking

---

[91] *See* Comments of the Telecommunications Industry Association, WC Dkt No. 07-52 *et al.*, at 23 (filed Feb. 13, 2008) (filed in response to *Comment Sought on Petition for Declaratory Ruling Regarding Internet Management Policies*, Public Notice, 23 FCC Rcd 340 (2008); *Comment Sought on Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators*, Public Notice, 23 FCC Rcd 343 (2008)).

[92] As Atkinson and Weiser comment: "To the extent that [broadband usage policies are transparent], it is quite possible that the most effective protection for consumers will be their own vigilance about what services network providers offer them. To facilitate such vigilance, all providers should be required to state clearly to what extent content and services enjoy preferential delivery opportunities and to what extent limitations exist on the ability of consumers to access the content and services of their choice." Robert D. Atkinson and Philip J. Weiser, *A Third Way on Network Neutrality*, The New Atlantis (Summer 2006) ("*A Third Way*").

[93] *NPRM* at ¶118.

[94] *Id.* at ¶119.

[95] *Id.* at ¶127.

for the Commission, particularly given the burden on providers. For example, in their attached declaration, Kenneth Ko and Kevin Schneider state that "[i]t is critical for the security of all network users that any requirement to disclose information concerning network management practices be tempered by the need to maintain security against the malicious attacks, malware, phishing, spam, and other threats that network providers must fight on a continuous basis."[96] As Ko and Schneider point out, "[a]ttackers can and will use any detail provided under regulatory disclosure in their attempts to breach network security measures."[97]

The Commission also proposes a far-reaching government reporting regime with little explanation or basis: "We seek comment on the frequency and content of any reports from broadband Internet access service providers that would make open Internet policies enforceable and/or provide a useful tool for policy making."[98] The Commission even seeks comment on whether providers shall be required to report the "number and content of any consumer complaints about the adequacy of disclosure both pre- and post-sale" as well the same information for "complaints filed by content, application, and service providers."[99] This is an unusually broad effort, and potentially puts the Commission in the burdensome role of policing provider notifications for little obvious reason. Absent evidence of repeated and demonstrable harm resulting from improper notification, it is difficult to understand why the Commission would endeavor to put in place such a reporting regime without a more significant cost-benefit analysis. Even more troubling is the suggestion that providers might be placed in the position of obtaining preclearance before utilizing a particular management practice. As Ko and Schneider state:

---

[96] Ko/Schneider Declaration at 20.

[97] *Id.* *See also* Tooley/Bowman Declaration at 24.

[98] *NPRM* at ¶128.

[99] *Id.*

> Network security is a constantly evolving struggle, as new malware and viruses are introduced at an alarming rate. As an example, any user of modern antivirus software has probably observed that, while in years past antivirus tools downloaded new virus definitions once a week, the cycle time for updates is now measured in *minutes*. Under these rapidly changing conditions, hampering network providers with requirements for pre-notification of detailed changes – or, even worse, requiring pre-*approval* of those changes – would create a situation ripe for disaster.[100]

TIA also is concerned with the *NPRM*'s suggestion of standardized disclosure requirements. For example, the Commission seeks comment on "standard labeling formats," "what events should trigger disclosure obligations," and whether or not "broadband Internet access service providers [should] be required to disclose any changes to their network management practices before or within a certain period of time after implementing those changes."[101] These questions are highly intrusive into the customer-provider relationship and could hamper the ability of providers to compete on issues of marketing and customer notification.

TIA has consistently supported a consumer-based disclosure principle, and urges the Commission to consider this option.[102] Ultimately, though, the Commission must carefully weigh the goal of codifying a far-reaching transparency principle against the potential harms it could cause to the management of the underlying network.

---

[100] *See* Ko/Schneider Declaration at 20.

[101] The *NPRM*'s suggestion of requiring prior notification is particularly troubling, insofar as network management decisions and techniques occur on a dynamic basis in reaction to constantly evolving new threats (*e.g.*, viruses, denial of service attacks) and unanticipated congestion. Network operators cannot wait for hours, days, weeks or months for any requisite "notice of change" to take effect.

[102] As previously discussed, TIA was a member of the HTBC, which first set forth broadband "connectivity principles" over six years ago. First among these was a principle stating that "[c]onsumers should receive meaningful information regarding their broadband service plans." *See HTBC September 2003 Letter*.

B. In The Event It Adopts Neutrality Rules, The Commission Must Frame Its Proposed Exceptions Broadly To Ensure Continued Innovation And Investment In Broadband Infrastructure

Modern broadband networks require intensive network management. Absent such management, the use of high-bandwidth applications such as VoIP, streaming video, video conferencing, and gaming would be constrained or infeasible.[103] If the Commission determines to go forward with network management rules, it must ensure that its proposed "exceptions" to a codified nondiscrimination principle afford sufficient flexibility to broadband service providers and manufacturers so that they can develop and operate products that maximize the customer's broadband experience. Ultimately, many allegedly discriminatory policies are in fact grounded in sound network management practices and should be permitted.

1. The Commission must adopt an expansive and flexible definition of "reasonable network management" that reflects the functionality of contemporary broadband networks

Growing traffic demands require that providers retain flexibility to employ a robust and diverse set of traffic-management tools. The *NPRM* appears to recognize as much:

> First, we propose that a broadband Internet access service provider may take reasonable steps to reduce or mitigate the adverse effects of congestion on its network or to address quality-of-service concerns. What constitutes congestion, and what measures are reasonable to address it, may vary depending on the technology platform for a particular broadband Internet access service.[104]

While the Commission may believe its rules and exception for reasonable network management will be accommodating, it should make every effort to ensure that it offers as much flexibility as possible so that providers truly are able to offer the best customer service possible. Said

[103] *See* Ko/Schneider Declaration at 19-20; Tooley/Bowman Declaration at 16-18.

[104] *NPRM* at ¶137.

differently, it would be a mistake for the Commission to adopt an approach with only a very limited exception and a presumption that anything else is unreasonable.

Any approach adopted by the Commission must account for the need for robust yet reasonable network management in the face of growing demand on the network and the growing use of applications sensitive to latency, jitter and packet loss.[105] Network providers employ management tools to enhance their typical users' experience without burdening those users with the costs of the additional capacity enhancements that would otherwise be necessary.[106] Moreover, these tools will become increasingly sophisticated as the demand for capacity keeps growing and technology continues to evolve. For these reasons, an exception that is drawn too narrowly would necessarily be based on today's perceptions of: what the Internet is; what the broadband Internet access market looks like; what consumers expect from their providers; what obligations should properly fall on users and applications providers; what is feasible or commonly employed in one particular technological platform; and so forth. These current conceptions, however, are unlikely to reflect technical and market developments over the coming years – as demonstrated by the fact that broadband deployment and Internet usage figures have consistently matched or outpaced the growth rate of other significant technologies.[107]

Finally, it is important to note that increased network demand is not the only legitimate justification for reasonable network management. Subscribers expect network operators to block an assortment of harmful or otherwise undesirable content, including spam, spyware, denial of

[105] *See* Tooley/Bowman Declaration at 12, 16-18; Ko/Schneider Declaration at 19-20.

[106] *See* Tooley/Bowman Declaration at 4, 16; Ko/Schneider Declaration at 21. *See also NPRM* at ¶136 ("it may be reasonable for a provider to take measures to counter traffic that is harmful or unwanted by users").

[107] "With home broadband penetration clearly on track to break 50 percent by the end of 2007, it will have taken nine years from the time the service became widely available for home high-speed to reach half the population. To put this in context, it took 10 years for the compact disc player to reach 50 percent of consumers, 15 years for cell phones, and 18 years for color TV." Gary Kim, *U.S. Broadband: Normal S Curve*, *available at* http://www.ipbusinessmag.com/departments/article/id/344 (last visited Jan. 8, 2010).

service attacks, viruses, and (in the case of ISP-managed parental controls) indecent or violent materials.[108] In all of these cases, reasonable network management plays a critical and beneficial role in shaping the user's experience to his or her preferences.

2. The Commission must recognize the important role being played by managed and specialized services, and must design any new rules to ensure that such services continue to flourish

In the *NPRM*, the Commission is right to recognize the consumer benefits of managed and specialized services and to view these services with regulatory caution.[109] These services differ from "plain-vanilla" best efforts broadband Internet access and highlight the shortcomings of a simple "non-discrimination" rule. Any steps toward regulation would be likely to have the unintended consequence of freezing the innovation that is the hallmark of these valuable services, contrary to the public interest.

Definition. Although all services that fall within the umbrella of the "managed" or "specialized services" label may share some common traits and characteristics, the Commission should proceed cautiously as it considers a definitional framework for these services.[110] In considering a definition, the Weldon Declaration makes clear that "we are entering a period of tremendous change in the definition of managed services" and, as a result, "there is a very real risk that any attempt to explicitly and narrowly define what is a 'Managed Service' or to limit the number or variety of such services that are permitted, will seriously miss the mark and stifle

[108] *See* Tooley/Bowman Declaration at 20, 22; Ko/Schneider Declaration at 23.

[109] *NPRM* at ¶¶148-53. Specifically, the Commission notes that the "existence of [managed and specialized] services may provide consumer benefits, including greater competition among voice and subscription video providers, and may lead to increased deployment of broadband networks." *Id.* at ¶148.

[110] *Id*. at ¶151 (asking "how should we define the category of managed or specialized services?").

innovation."[111] Thus, to the extent the Commission considers defining managed or specialized services at all, it should only do so in the broadest possible way.

To date, policymakers have principally identified managed and specialized services by example. In the *NPRM*, the Commission highlights AT&T's UVerse, eLearning, telemedicine and smart grid applications as examples of managed and specialized services.[112] Similarly, in their consideration of managed services, the National Telecommunications and Information Administration ("NTIA") and the Rural Utilities Service ("RUS") chose only to define managed services by example, citing to telemedicine, public safety communications, and distance learning, which use private network connections rather than the public Internet.[113] Commenters before the FCC have variously labeled the following as managed and specialized services: teledentistry, telepharmacy, telepsychiatry, remote patient monitoring, Metro Ethernet, wireless, VoIP, data center services, and disaster recovery center services.[114] Indeed, the Weldon Declaration also provides a number of examples of managed service offerings across the consumer, enterprise, education and government sectors.[115] As individual business, government and consumer requirements differ greatly, so, too, do the characteristics of what many consider to be managed and specialized services. Managed services generally require one or several of the following elements: (i) guaranteed (low) packet loss; (ii) guaranteed (low) packet delay; (iii)

[111] Declaration of Marcus Weldon at 9 ("Weldon Declaration"). *See also* Ko/Schneider Declaration at 23.

[112] *NPRM* at ¶150.

[113] Broadband Initiatives Program; Broadband Technology Opportunities Program Notice, 74 Fed. Reg. 33104, 33111 (July 9, 2009) ("*Broadband NOFA*").

[114] *See* Comments of Internet2, GN Docket Nos. 09-47, 09-51, 09-137, WC Docket No. 02-60, at 14 (filed Dec. 2, 2009); Comments of Alcatel-Lucent, GN Docket Nos. 09-47, 09-51, 09-137 at 11 (Dec. 4, 2009); OneCommunity, Ex Parte Presentation, GN Docket Nos. 09-47, 09-51, 09-137 (filed Nov. 11, 2009).

[115] *See* Weldon Declaration at 2-3.

secure, private connectivity; and (iv) guaranteed bandwidth.[116] These attributes are not universal, however, further complicating efforts to define managed services.[117]

In addition, different managed and specialized services may reside at different places within and across different networks in the future. For example, the Weldon Declaration notes that most current managed services are created by operators for serving an established need on the part of the end user entity. A second, emerging category of managed services are requested directly by the end consumer as a result of an enhanced QoS need and represent a far more diverse array of services (*e.g.*, cloud computing and web content delivery).[118] Whereas the first category of services are generally provided over managed IP networks, the second category would be delivered over the public Internet to the edge of the operator network, at which point the services will take advantage of the typical managed IP delivery architecture.[119] Moreover, while certain managed service suites require on-site equipment and active management, others only require that the service provider supply connectivity. Ultimately, though common traits can be identified (*e.g.*, high QoS, minimal packet loss or delay), for overarching "categories" of managed and specialized services, such services are hard to satisfactorily capture with any single, dynamic definition.

Operation. A review of some managed services used in the business sector can be instructive to help understand their operation and utility for businesses.[120] As companies

---

[116] *See id*. at 1-2.

[117] *See id*. at 2-3. For example, audio communications services require minimal packet delay and a minimum bandwidth guarantee but may not have stringent packet loss requirements. In contrast, video communications do require minimal delay, a bandwidth guarantee and low packet loss.

[118] *See id*. at 5.

[119] *See id*.

[120] As illustrated in the Weldon Declation, there may be a number of ways in which a managed service can provide traffic flow control. Typically, packets are classified at the point of ingress to the managed service network, policed according to certain parameters, and then marked for forwarding in a specific class. This forwarding class is

transition to all-IP networks, managed services have become essential to the success of everyday business operations as well as critical business functions.[121] Managed services can include software, hardware and other IP networking services that are designed to suit the individual needs of the users and their business requirements. Viewed broadly, managed services can improve a company's business processes and allow it to focus on its core competencies by removing worry about network technologies, management, and capital investments.

By way of example, some companies use managed IP communications services like site-to-site voice in order to allow for seamless communications between distant offices. A site-to-site voice service allows the different office locations to call one another through a VoIP infrastructure. Meanwhile, other companies may employ managed services like telepresence and web collaboration to connect distant offices and employees. Similarly, companies use voice over virtual private network ("VPN") managed services to allow their telecommuters and mobile workers to communicate effectively. These services can result in large cost-savings for companies.

Benefits and Regulatory Consequences. It is important for the Commission to recognize the numerous benefits that managed services currently offer to American consumers and the U.S. economy. Managed services provide potentially life-saving benefits in the form of telehealth, entertainment options like IPTV or online gaming, and energy savings through the use of remote home monitoring. For government and public users, managed services can provide necessary

---

mapped to a specific queue type in the network element. The packets in the queue are then 'de-queued' according to well-defined algorithms that minimize the packet loss and delay associated with the different service flows. *Id*. at 6.

[121] Managed services are critical to resolving quality of service, bandwidth availability and security concerns. According to one study, one hour of system downtime can cost a company between $330,000 and $2.8 million. *See* Cisco Guide to Buying Managed Services, *available at* http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns465/net_brochure0900aecd8019efd7.pdf (last visited Dec. 11, 2009).

QoS and security protections for services like public safety communications.[122] For businesses, managed services can reduce and stabilize costs, including IT operations and transport expenses; increase ease of communication; promote efficient business practices; provide access to the latest technology with limited risk; and make it easier to adapt to changing business conditions. To these ends, managed services also act as a driver for marketplace expansion and network innovation.[123]

In turn, global markets as well as the U.S. workforce and citizenry expect that their specialized and managed services will work in an uninterrupted and timely fashion. There is simply little to no tolerance for latency, jitter, packet loss or lack of availability for these business or mission critical services. A misguided decision to impose network management rules, particularly non-discrimination, on managed services would severely undermine the utility of managed services.[124]

More specifically, any network management rule would lie in tension with the fact that many managed services are deliberately offered outside of the best-effort Internet due to the value or sensitivity of the content. For instance, in the case of IPTV, a mandate to access the content from outside of the managed service could compromise the service's security and integrity.[125] Moreover, a managed service by definition "offers the end user content, applications and services in a manner that has a higher level of QoS when compared to best effort broadband

[122] National Broadband Plan Policy Framework, December 16, 2009 – FCC Open Meeting, at 33-34 , available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-295259A1.pdf (noting National Broadband Plan goals and options relating to public safety, including "preserve broadband communications during emergencies.").

[123] The research firm Ovum has projected that the market for four managed services - Managed Metro Ethernet, Virtual Private Network, Voice and Security Services – will reach $66 billion in 2012. *See, e.g.*, Press Release, Cisco, Ovum Projects $66 Billion Market for Four Managed Services by 2012 (May 19, 2008), *available at* http://newsroom.cisco.com/dlls/2008/prod_051908b.html.

[124] *See* Weldon Declaration at 10-12.

[125] *Id*. at 11.

Internet access service," which is in direct tension with proposed network management rules.[126] Finally, and possibly in direct conflict with the Commission's proposed transparency principle, managed services are offered as complete products to end users, and the network management and security tools used therein may be proprietary, such as those used for traditional VPN services. Required disclosure of managed services protocols and other sensitive information could compromise the QoS or security guarantees that are essential to the viability of managed and specialized services.[127]

To be clear, managed and specialized services promote the public interest; they do not harm or threaten the public Internet. As the Commission contemplates managed services in this proceeding, it must recognize the innovations that managed services have begun, and will continue, to yield. The Weldon Declaration makes clear that services providers' business plans depend on both robust managed services as well as high speed Internet.[128] To date, managed service offerings have peacefully coexisted with and complemented the public Internet, and there is no evidence that this balance is at risk. As the Commission moves forward with this proceeding, TIA urges it to cautiously approach the subject of managed services so as to ensure that they continue to be allowed to flourish in this developing marketplace.

3. The Commission must ensure that providers remain able to navigate the important demands of law enforcement, public safety, and homeland/national security

Any network management rules must not impact the ability of broadband Internet access service providers and infrastructure manufacturers to adequately respond to the needs of law

[126] *Id*. at 12.

[127] *Id*. at 12-13.

[128] *Id*. at 5.

enforcement, public safety, and homeland security.[129] The Commission should adopt an exception to guarantee "quality of service" for matters that "may be critically important to our national security and safety."[130]

The need for a homeland security exception highlights the significant regulatory uncertainty that will be caused by a Commission decision to adopt network management rules. While a homeland security exception is laudable, it cannot completely resolve the potentially negative impact that network management rules will have on matters of homeland security. The bottom line is that in codifying the *Policy Statement* and adding rules on non-discrimination and transparency, the Commission would severely impact the flexibility that has allowed providers and manufacturers to manage the network for the benefit of the homeland security community when appropriate.

While the Commission is right to put this exception in place, the mere presence of network management rules will cause unnecessary delay as providers will need to ensure that their actions truly are permitted under the homeland security exception. Yet, the need for immediate network management is particularly acute during emergency situations.[131] Important time could be lost as providers work through questions such as who is declaring the "emergency" situation, how long will the emergency last, and what the consequences are if management tools

[129] TIA members routinely work on issues of importance to the law enforcement, public safety and homeland security communities. For example, TIA members have worked closely on matters regarding the interoperability of wireless public safety networks, enhanced 911 and public safety funding. *See, e.g.*, Letter from Grant Seiffert, President, Telecommunications Industry Association, to The Honorable John D. Rockefeller, IV, The Honorable Kay Bailey Hutchinson, and The Honorable Jane Harman (Oct. 6, 2009) (supporting legislation to extend the funding for the Public Safety Interoperable Communications grant program through 2012); Comments of Telecommunications Industry Association, PS Dkt No. 07-114, CC Dkt No. 94-102, WC Dkt No. 05-196 (filed Aug. 20, 2007) (comments in E911 location accuracy proceeding); Letter from Grant Seiffert, President, Telecommunications Industry Association, to The Honorable Patrick Leahy and The Honorable Jeff Sessions (May 12, 2009) (supporting S. 167, the "COPS Improvements Act of 2009").

[130] *NPRM* at ¶145.

[131] *See* Tooley/Bowman Declaration at 25; Ko/Schneider Declaration at 21.

remain in place after an actual event is officially concluded.[132] These concerns could be significant and point out a basic weakness in adopting network management rules.

C. Any Rules Adopted Must Recognize The Important Distinctions Among Different Broadband Platforms, And The Ways In Which These Distinctions Affect Network Management Requirements

TIA has long believed that technologies should succeed or fail on their merits, not on the support of or lack thereof government regulation.[133] Thus, as it considers the issues posed in this proceeding, TIA urges the Commission to ensure that it does not take action that will significantly (and negatively) impact one broadband platform over another. As set out above, if the Commission continues to rely on the more flexible *Policy Statement*, providers can implement network management techniques – consistent with the four principles – that best apply to the network at hand. However, since the Commission is considering whether to impose rules that will restrict the ability of providers to act in certain circumstances, it is important that the Commission not ignore the distinct aspects of the various technology platforms and that it ensures that one platform is not significantly disadvantaged over another by whatever rules are adopted.[134]

---

[132] *See, e.g.*, *NPRM* at ¶145 ("For example, during a *public health emergency*, increased absenteeism and utilization of teleworking would likely increase the number of users seeking to access the Internet from numerous discrete points (*e.g.*, residences).") (emphasis added).

[133] *See, e.g.*, Comments of the Telecommunications Industry Association, In the Matter of American Recovery and Reinvestment Act of 2009 Broadband Initiatives, Docket No. 090309298-9299-1, at 10-11 (April 10, 2009) (*TIA BTOP/BIP Comments*") ("Additionally, to generate the maximum benefit of broadband funds available, NTIA and RUS should take a technology-neutral position on grant awards so that all innovative technologies can be included in the BTOP and RUS programs. All forms of broadband service – wireline, wireless (of all types), satellite, or a combination thereof – offer distinct qualities that render them useful in different circumstances and regions.").

[134] In the BTOP/BIP process, NTIA and RUS ensured that their rules did not obviously disadvantage one technology over another – thus, for example, the Notice of Funds Availability did not require mobility as a condition for broadband funding, nor, in the alternative, did it require a minimum broadband speed that could only be met by wireline networks. "NTIA expects to distribute grants across geographic areas addressing these various public purposes. It will issue awards on a technologically neutral basis, and expects to support projects employing a range of technologies (e.g., fixed and mobile wireless, fiber, satellite)." *Broadband NOFA*, 74 Fed. Reg. at 33107 (July 9, 2009).

Any approach to network management must recognize that each provider will utilize specific management tools depending on their network and operational situation. Thus, in attempting to limit possible "violations" of any new network management rules, the Commission must realize that perceived violations are likely to turn on fact-specific questions regarding the precise benefit of specific network management practices and the precise costs imposed by those practices – for example, whether the network management practice at issue is "reasonable" with respect to the particular network and operational situation. The answers to this initial set of questions likely will turn on a number of related technical and network specific questions: What is the specific capacity of the network at the last mile; in all relevant points in the backbone? How fully is such capacity being utilized at different times of day, on different days of the week? What is the best way to protect latency- and jitter-sensitive traffic while minimizing any harm to other traffic? Which traffic warranted special treatment, and when? What factors should have been considered in prioritizing traffic? The answers to each of these questions could be different depending on the broadband network at issue.

The Commission should not attempt to provide guidance or rules that are based on any one network or platform, because that could result in policies that put other networks and platforms at a disadvantage, contrary to the Commission's longstanding commitment to technology-neutral policies.[135] For example, there may be significant differences among the scheduling algorithms used for allocating bandwidth resources among contending users on cable,

[135] *See, e.g.*, Bringing Rural Broadband to America: A Report on Rural Broadband Strategy, 24 FCC Rcd 12791, 12800 (2009) (noting that, in assessing rural broadband, "decision makers should proceed on a technology-neutral basis--by considering the attributes of all potential technologies--in selecting the technology or technologies to be deployed").

wireless, and fiber platforms, based on the unique characteristics of the various platforms, and any one of the algorithms may be wholly unsuited to other platforms.[136]

Ultimately, these are dynamic questions of technology, not policy, and their answers will change over time as technology evolves. Consequently, the Commission must ensure that any rules it adopts in this proceeding account for the differences in broadband network platforms and ensure that one platform is not particularly disadvantaged by the adoption of specific network management rules.

D. Enforcement Should Be Case-By-Case And Narrowly Tailored To Cure The Harm

In view of the many flaws associated with *ex ante* prohibitions on specific network-management techniques, the Commission should rely on case-by-case adjudications rather than adopt specific rules and procedures.[137] This would be consistent with the Commission's approach to evaluating alleged violations of the "just and reasonable" requirements set forth in sections 201(b) and 202(a) of the Act. Case-by-case adjudications should also allow for the Commission to focus on a specific allegation of misconduct, which will provide for more timely resolution. This is an especially important consideration given the real-time environment of network management and the highly dynamic status of the underlying network.

A case-by-case review also will permit a more thoughtful, calibrated approach to network management that is responsive to changing market and technological conditions yet still is capable of addressing specific conduct that warrants punishment. As Atkinson and Weiser observed:

---

[136] As discussed above, wireless mobile data networks typically use proportionally fair scheduling, which balances the quality of each data flow against network efficiency in the interest of a satisfactory customer experience. A different approach may be appropriate in an environment where transmission quality is the same for each data flow.

[137] *See NPRM* at ¶176 ("We seek comment on whether the Commission should adopt procedural rules specifically governing complaints involving alleged violations of any Internet principles we codify in our regulations.").

> The problem with rules that limit behavior before-the-fact is that they often sweep broadly and address speculative harms. Moreover, such rules create incentives for gamesmanship, such as an effort to have a video-over-Internet service classified as a 'cable service' and thus outside the scope of any network neutrality regulations. By contrast, an after-the-fact approach provides regulatory flexibility, viewing discriminatory conduct by providers with market power with a degree of skepticism, but judging such conduct on a case-by-case basis."[138]

As explained above, TIA believes that a broad reasonable network management exception is critical to allow service providers and infrastructure manufacturers to efficiently manage their continually evolving broadband networks. But, the Commission also should recognize that "reasonable network management" tools may vary from provider to provider depending on the provider's network technology and other operational issues. A case-by-case approach allows the Commission to focus on the specific facts at issue, *e.g.*, the provider, the alleged violation, the impact on competition, the network technology, the relationship between the alleged violations and the underlying network, operational considerations, and many other key factors. This review is an inherently subjective one and thus is best served by a regulatory construct that allows the Commission flexibility to deal with the specific allegation at hand. Moreover, given the real-time nature of network management and the ongoing technological evolution of management tools, a case-by-case approach to alleged improprieties will be most effective in policing providers' practices on an ongoing basis.[139]

Nor would a case-by-case approach be at all novel or unusual. The Commission and the courts have recognized that individual adjudication is the best means for evaluating claims of anticompetitive activity. Thus, for example, the Commission has generally evaluated claims that providers have engaged in unjust or unreasonable behavior in the context of dispute-specific

[138] *See A Third Way* at 56.

[139] *Id.*

adjudications.[140] Indeed, the Commission already has dealt with the single alleged violation of the *Policy Statement* in a similar fashion.[141] In the *Comcast Order*, for example, the Commission "decline[d] to adopt prophylactic rules," citing its intent "to adjudicate disputes regarding federal Internet policy on a case-by-case basis."[142] The Commission noted that the case-by-case approach was most consistent with "federal policy advocat[ing] the preservation of the 'vibrant and competitive free market' for Internet and interactive computer services."[143] Finally, over the past century, the courts also have developed a case-by-case approach used to adjudicate most claims of anticompetitive conduct, recognizing that decision-makers must evaluate the net effects of a particular practice.[144]

[140] *See, e.g., Business Discount Plan, Inc.*, Order on Reconsideration 15 FCC Rcd 24396, 24399 (2000) ("In enacting section 201(b), Congress did not enumerate or otherwise limit the specific practices to which this provision applies. Instead, it granted us a more general authority to address such practices as they might arise in a changing telecommunications marketplace."); *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, Third Report and Order and Third Further Notice of Proposed Rulemaking,17 FCC Rcd 14860, 14917 (2002) ("For conduct to be unlawful under section 201, the Commission must find that the conduct is 'unjust or unreasonable.' We believe that this standard requires a review of case-specific facts….").

[141] *See Comcast Order*.

[142] *Id.*, 23 FCC Rcd at 13045-46.

[143] *Id.* at 13046. Commissioner Copps explained that he "ha[d] long advocated … a case-by-case analysis of the facts in particular cases," and then-Commissioner Jonathan Adelstein applauded the "flexibility" afforded by the FCC's "case-by-case approach." *Id.*, Statement of Commissioner Michael J. Copps; *id.*, Statement of Commissioner Jonathan S. Adelstein.

[144] *See, e.g., Board of Trade of the City of Chicago et al. v. United States*, 246 U.S. 231 (1918).

III. CONCLUSION

For the foregoing reasons, TIA encourages the Commission to take action in this proceeding consistent with the recommendations set out above.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: _____

Danielle Coffey
Vice President, Government Affairs

Rebecca Schwartz
Director, Regulatory and Government Affairs

Patrick Sullivan
Director, Technical and Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

January 14, 2010