

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

In the Matter of)	
)	
New Part 4 of the Commission's Rules Concerning Disruptions to Communications)	ET Docket No. 04-35
)	
Consumer Protection in the Broadband Era)	WC Docket No. 05-271
)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as amended by the Broadband Data Improvement Act)	GN Docket No. 09-137
)	
A National Broadband Plan For Our Future)	GN Docket No. 09-51
)	
International Comparison and Survey Requirements in the Broadband Data Improvement Act)	GN Docket No. 09-47
)	

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

Neal M. Goldberg
Loretta P. Polk
Steven F. Morris
Jennifer K. McKee
Counsel for the National Cable &
Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

August 2, 2010

Table of Contents

INTRODUCTION AND SUMMARY2

I. THE COMMISSION SHOULD CAREFULLY CONSIDER WHETHER VoIP AND BROADBAND OUTAGE REPORTING REQUIREMENTS ARE NECESSARY IN LIGHT OF TODAY’S ROBUST BROADBAND NETWORKS4

II. THE COMMISSION SHOULD NOT SIMPLY EXTEND EXISTING OUTAGE RULES TO NEWER INTERNET PROTOCOL-BASED TECHNOLOGIES THAT OPERATE IN A COMPLEX INTERNET ECOSYSTEM7

III. THE COMMISSION SHOULD ENCOURAGE VOLUNTARY INDUSTRY EFFORTS AND FACILITATE MECHANISMS FOR INDUSTRY TO WORK TOGETHER TO DEVELOP AND SHARE BEST PRACTICES TO AVOID SERVICE DISRUPTIONS11

CONCLUSION.....13

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

In the Matter of)	
)	
New Part 4 of the Commission’s Rules Concerning Disruptions to Communications)	ET Docket No. 04-35
)	
Consumer Protection in the Broadband Era)	WC Docket No. 05-271
)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as amended by the Broadband Data Improvement Act)	GN Docket No. 09-137
)	
A National Broadband Plan For Our Future)	GN Docket No. 09-51
)	
International Comparison and Survey Requirements in the Broadband Data Improvement Act)	GN Docket No. 09-47
)	

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association (“NCTA”) hereby submits its comments in response to the Public Notice (“*Notice*”) issued by the Commission on July 2, 2010 in the above-captioned proceedings.¹

¹ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation’s cable television households and more than 200 cable program networks. The cable industry is the nation’s largest provider of high-speed Internet service (“broadband”) after investing over \$160 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to over 20 million customers.

INTRODUCTION AND SUMMARY

In the *Notice*, the Public Safety and Homeland Security Bureau seeks comment on whether the Commission's rules concerning disruptions to communications or "outages" should be extended to broadband Internet service providers (ISPs) and interconnected Voice over Internet Protocol (VoIP) service providers. The current rules apply to circuit-switched voice and/or paging communications over wireline, cable and satellite communications services.

The *Notice* arises from the Commission's National Broadband Plan, which recommended that the Commission initiate a proceeding to consider extending Part 4 outage reporting rules to ISPs and VoIP providers in order to "allow the FCC, other federal agencies and, as appropriate, service providers to analyze information on outages affecting IP-based networks."² It envisions using the information to help prevent future outages, promote better responses to actual outages, and help protect against cyber attacks.

Expanding the existing network outage reporting regime to interconnected VoIP and broadband ISPs raises significant – and complicated – issues as to whether, and if so how, such rules should be applied to these services.

First, the complex network infrastructure required to support the diverse needs of broadband communications – video, voice, data for fixed and mobile use – has led to the development of robust networks designed to withstand failures and minimize the effect on customers. Disruptive incidents are infrequent and of short duration because of the many redundancies and safeguards built into the networks. In part this is due to the increasingly competitive marketplace in which all providers operate, which provides enormous incentives for companies to ensure that their networks can withstand physical harm, severe loads, and other

² CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN, rel. March 16, 2010 ("Plan") at 321.

stresses. Under such circumstances, it should not be a foregone conclusion that VoIP and broadband network outage reporting is necessary.

Second, IP-based networks and circuit-switched networks are so different that a variety of factors need to be explored before simply expanding the existing regulatory structure to VoIP and broadband Internet services. The impact of significant technology and marketplace changes that have occurred since the Commission last adopted outage rules needs to be fully considered as well.

Third, today's broadband communications are characterized by a complex web of entities providing a wide array of inter-connected functions, including not just broadband Internet access facilities but content delivery networks, application providers and others. VoIP and broadband ISPs may not control the root cause of an outage or may need more time than is required on a circuit-switched network to diagnose the problem and determine the specific number of customers affected. The global nature of the Internet – and of threats to network survivability and continuity of service – underscores that outage reporting by just broadband ISPs will provide an incomplete picture of outages.

Fourth, the existing voluntary public-private sector framework has resulted in mutually beneficial information-sharing mechanisms and the implementation of programs to maintain a reliable and resilient communications infrastructure. The Commission should look to these ongoing efforts to combat outage threats and incidents in evaluating the need for VoIP and broadband Internet outage regulation.

I. THE COMMISSION SHOULD CAREFULLY CONSIDER WHETHER VoIP AND BROADBAND OUTAGE REPORTING REQUIREMENTS ARE NECESSARY IN LIGHT OF TODAY’S ROBUST BROADBAND NETWORKS

In considering whether to pursue a new regime of network outage reporting for VoIP and broadband, the Commission should first recognize that a network “outage” in the context of modern packet-switched broadband networks is a vastly different issue than an outage in the context of traditional circuit-switched networks. As described in NCTA’s recent submission in the network survivability proceeding, today’s broadband networks are robust and resilient by “design.”³ They have the ability in most circumstances to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.⁴ The physical network infrastructure contains a host of redundancies to prevent service outages, such as redundant fiber rings, routers and optical node receivers. The routing and rerouting of information occur automatically to avoid disruptions, congestion and failures in connectivity.

Moreover, these architectural elements enable broadband network providers to mitigate the cascading effects of disruptions to their networks and ensure that such incidents affect the smallest geographic area as possible. And even in the case of regional and local network disruptions, broadband network operators have designed their systems with substantial safeguards that minimize the impact of failures and promote reliable, uninterrupted service to their customers. With very few single points of failure in the network, any single failure not only

³ United States Dep’t of Homeland Security, *Communications Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* at 34, 88 (May 2007) (“DHS Communications Sector-Specific Plan”), available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf>. The United States Government Accountability Office (GAO) reported based on the Sector-Specific Plan that “resiliency is achieved by the technology, redundancy, and diversity employed in network design and by customers who employ diverse and resilient primary and backup communications capabilities, thereby increasing the availability of service to customers and *reducing the impact of outages*”. *Critical Infrastructure Protection, Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience* at 25, GAO-10-296 (Mar. 2010) (citing the DHS definition of “resiliency”) (“GAO Critical Infrastructure Report”) (emphasis added).

⁴ GAO *Critical Infrastructure Report* at 4.

impacts as few customers as possible but can normally be remedied quickly. When faced with physical damage or severe overload conditions, the network is often capable of self-healing through a variety of means, such as dynamic routing (both within backbones and between different backbone networks); backup and redundant power; and multiple access points to reach fiber and other facilities.⁵ Moreover, equipment and systems are monitored 24 hours a day, seven days a week to identify and prepare for threats to network operations.⁶

While fiber cuts, traffic overloads and disaster situations are unpredictable, they are a normal part of business and broadband network operators are able in most instances to manage such conditions in a manner that maintains quality and is transparent to the end user. Wide scale outages due to network failures have become increasingly rare. That does not mean that a catastrophic event could not bring down a broadband network, but the necessity and value of extending the current Part 4 outage reporting requirements to broadband networks merits a close look in light of today's robust networks.

In that regard, as an initial step, it might be useful for the Commission to undertake a comprehensive examination of the manner in which it uses the outage data it already collects and how additional data would be used. In the *Notice*, the Commission states that it uses the information submitted pursuant to Part 4 of its rules to, among other things, "address communication system vulnerabilities and help prevent future disruptions." Similarly, the

⁵ For a full description of the cable broadband network's fundamental architectural elements and infrastructure design that promote resiliency and avoid outages, see Comments of the National Cable & Telecommunications Association, PS Docket No. 10-92 (filed June 25, 2010) ("NCTA Survivability Comments") at 6-10.

⁶ As described by Comcast, for example, in the network survivability proceeding, active monitoring, ticketing and reacting occur promptly through various tools used round-the-clock by network operations personnel. Key network segments are regularly tested as a precaution and to diagnose issues in real time. Comcast also noted that when failures do occur, typically the link going down will trigger a routing update and within one second the traffic will have found a new path to the destination. In rare cases, a link may fail without triggering a "link down" event. When that happens, it typically will take the broadband network approximately six seconds to recognize the failure on its own and route around the failed link. See Comments of Comcast, PS Docket No. 10-92 (filed June 25, 2010) at 11.

National Broadband Plan envisions using VoIP and broadband data to help prevent future outages, promote better responses to actual outages, and help protect against cyber attacks.⁷

These are worthy goals but are stated so generally that they do not provide a meaningful basis for considering whether there is a need to extend the requirements as proposed. Therefore, NCTA recommends that, before imposing additional reporting requirements and consistent with Chairman Genachowski's vision of an open and transparent Commission, the Commission should prepare and release a report providing a detailed description of how it uses current outage data, what actions it has taken based on the data, and what conclusions, if any, it has drawn from the data to the extent they pertain to VoIP and broadband Internet services.

In addition, the Commission currently collects information from cable operators and other service providers on the status of communications networks during disaster situations under its Disaster Information Reporting System (DIRS). This information is furnished to federal officials seeking to assist communications providers in the midst of a crisis. But beyond severe disaster situations, which may result in physical damage, disruptions and power outages, the question should be asked: is there a significant issue with respect to network outages in the United States? Cable operators and other broadband network providers have shown that even during extreme weather conditions and other emergencies over the past decade, they can withstand peak usage of their networks over a sustained period. This was recently evidenced by the high performance of broadband networks during the record-breaking snowstorms and floods of the past winter and spring.

⁷ Plan at 321.

II. THE COMMISSION SHOULD NOT SIMPLY EXTEND EXISTING OUTAGE RULES TO NEWER INTERNET PROTOCOL-BASED TECHNOLOGIES THAT OPERATE IN A COMPLEX INTERNET ECOSYSTEM

The Commission last reviewed network outage issues six years ago.⁸ The significant technology and marketplace changes that have occurred since that time need to be fully considered before any further actions are taken in this area. In 2004, the various technologies that the Commission focused on – wireless and satellite communications – provided a *voice* communications service that resembled basic telephone service. Today, millions of people use services like Skype, Facebook, and Twitter to stay in touch with friends and family and an entire generation of teenagers communicates primarily by text messaging.

These changes have significant consequences on how consumers might be affected by outages. Because most consumers have multiple ways in which they communicate, *e.g.*, wireless and wireline subscriptions, an outage affecting only one of those services may be of less consequence than was the case in 2004. Moreover, outages for some of these new services may have a significant effect on consumers. As just one example, it is more likely that Facebook going down for an hour would have a much greater impact on the public than a small cable operator going down for an hour.

In light of all these changes, the Commission should not simply shoehorn VoIP and broadband Internet services into existing outage reporting standards. A variety of key factors should be explored in considering whether outage reporting is needed and, if so, what type of reporting is appropriate. These factors include, but are not limited to, the greater interconnected nature of broadband networks, applications providers and other entities that comprise the Internet, changing consumer expectations, technical characteristics of IP networks vs. circuit-

⁸ *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, ET Docket No. 04-35, 19 FCC Rcd 16830 (2004) (*Part 4 Order*).

switched networks, challenges of applying service-specific rules to a newer service, and the burdens and costs of reporting thresholds.⁹

For example, because of their robust nature and resiliency, VoIP networks are more complex than TDM-based networks, and it may be more difficult to identify the element or elements involved in a potentially reportable event. Furthermore, because IP packets carry various types of information (including video, voice, or other data) to and from different types of customers (including cable, VoIP, or others), it is difficult for a network provider to ascertain what kinds of packets have been affected by a failure of an “integrated” network element that handles various packet types. Moreover, because these commingled packets are dynamically routed over numerous Internet links, it is usually even more difficult to map the affected voice packets to particular customers to determine a footprint of voice customers affected by the failure. Thus, in most cases, the Commission cannot simply extend the current response time for reporting voice outages to VoIP services.

The challenge of determining the number of customers affected by an event, and the amount of time they are affected, is compounded if there are electric power outages. Because VoIP customer premises equipment depends on electric power, if there is an extended power outage (i.e., one that outlasts the battery backup capability of a VoIP phone), a customer may be unable to make calls even if the network itself is in working order. The same is true for homes that have traditional circuit-switched service but rely exclusively on cordless phones that depend on electric power. Indeed, because VoIP phones have battery backup capability, a household

⁹ The standard in the current outage rules is based on “user-minutes”, *i.e.* the general threshold for reporting an outage to the Commission is one that has (1) a duration of at least 30 minutes; and (2) it potentially affects at least 900,000 user-minutes.

subscribing to a VoIP service may be better positioned than a household taking circuit-switched service.

The complexity and inter-related nature of the Internet ecosystem warrants particular attention in the Commission’s analysis of disruptions in VoIP and broadband Internet services. As the Commission is well aware, the Internet infrastructure includes not only so-called “last mile” facilities, middle-mile transport and backbone facilities operated by Internet Service Providers, but content delivery networks (“CDNs”), server farms, and services operated by “application” providers. Given the nature of the threats to Internet communications – which are global in scope and pertain to applications to an even greater degree than to broadband facilities – the Commission should not overlook the significance of non-access networks in exploring outage issues.¹⁰

Indeed, consumers may experience outages when accessing the Internet via cable, wireline or wireless networks that not only are beyond the control of the broadband ISP, but beyond their knowledge. Customers purchasing services that ride “over-the-top” of broadband Internet networks may experience failures that are under the control of the over-the-top provider. Similarly, outages may result from failures in the Internet backbone that is outside of the broadband ISP’s facilities. In some cases, the broadband ISP may not even be able to locate the source of the outage or it may not immediately be able to determine whether or not particular customers can use their service.

¹⁰ See e.g., NCTA Survivability Comments at 18; *Cyber Security Certification Program*, PS Docket No. 10-93, NCTA Comments at 8-10 (July 12, 2010) (“NCTA Cyber Security Comments”). The National Institute for Standards and Technology (NIST) identified similar concerns in its recent Notice of Inquiry on cyber security. See *Cybersecurity, Innovation, and the Internet Economy*, Docket No. 100721305-0305-01, 75 Fed. Reg. 44216, 44219 (July 28, 2010) (explaining that inquiry will focus primarily on companies other than infrastructure providers).

Moreover, one of the main rationales in the National Broadband Plan for extending outage requirements to VoIP and broadband is to combat cyber attacks. However, most of the leading cyber threats today do not target the physical transmission layer. Cyber terrorists or hackers are much more likely to disrupt or shut down the application layer, such as social networking or e-mail, or gain access to personal or sensitive information through phishing attacks, rather than disrupt the underlying broadband access networks.¹¹ Services provided by broadband facilities are surely affected by attacks from botnets, malware, and spyware but reporting such disruptions will often not get at the root causes of such disruptions. Broadband facilities could remain up and running while broadband communications are halted by attacks affecting some other vulnerability in the Internet ecosystem.

In sum, if the Commission considers imposing outage reporting requirements on broadband ISPs, those providers should only be responsible for reporting outages caused by disruptions to their own facilities and should not be required to report (or otherwise be held accountable) for outages that are beyond their control or of which they may not even be aware.

¹¹ See, e.g., Ki Mae Heussner, *Watch Out: Cyber Threats to Expect in 2010*, ABC News/Technology, Jan. 1, 2010 (“Although consumers know to be wary of Web links sent by strangers, they tend to trust Web links and e-mail messages sent by friends and family. But online attackers are learning how to exploit that trust, by delivering malware that appears to come from Facebook friends, Twitter followers and friends’ e-mail accounts.”), at <http://abcnews.go.com/Technology/cyber-threats-expect-2010/story?id=9456824>; John Markoff, *Cyberattack on Google Said to Hit Password System*, N.Y. Times, Apr. 20, 2010 at A1 (describing cyber attack against Google).

III. THE COMMISSION SHOULD ENCOURAGE VOLUNTARY INDUSTRY EFFORTS AND FACILITATE MECHANISMS FOR INDUSTRY TO WORK TOGETHER TO DEVELOP AND SHARE BEST PRACTICES TO AVOID SERVICE DISRUPTIONS

The federal government has played and continues to play an important role in collaborating with private sector companies to develop methodologies and best practices to protect broadband communications networks.¹² This comprehensive public-private framework is addressing the ability of broadband communications networks to resist and recover from physical and other harm to network facilities and performance during natural and man-made disasters and other emergency situations. Work in this area has shown that the constantly evolving nature of broadband infrastructure and technology, as well as the content and applications available over broadband networks and on the Internet, requires flexible and nimble approaches to disruptive threats.

The Communications Security Reliability and Interoperability Council (“CSRIC”), for example, is charged with developing and updating best practices to ensure the availability of communications capacity during natural disasters, terrorist attacks, or other events that result in exceptional strain on the communications infrastructure. CSRIC’s mission also includes the identification of best practices to ensure and facilitate “the rapid restoration of communications services in the event of widespread or major disruptions.”¹³ CSRIC will provide recommendations to the Commission regarding best practices to ensure optimal security, reliability, and interoperability of communications systems, across all platforms – telecommunications, media and public safety communications systems.

¹² See NCTA Survivability Comments; NCTA Cyber Security Comments; *A National Broadband Plan For Our Future*, Comments of NCTA on PN #8 (Nov. 12, 2009).

¹³ Charter of the FCC’s Communications Security, Reliability, and Interoperability Council 1, available at http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf.

The emphasis on public-private initiatives has resulted in mutually beneficial information-sharing mechanisms and the implementation of programs to maintain a reliable and resilient communications infrastructure. The Commission should encourage affected segments of the industry to work together in cooperative, collaborative forums, such as CSRIC, and provide voluntary information to combat outage threats and incidents. Through these forums, the Commission can track general trends in disruptions to broadband networks and the state-of-the-art in best practices, and then determine if it needs to consider taking additional action. But, as we have seen, in a competitive marketplace, broadband service providers have enormous incentives to ensure that their networks have sufficient redundancy, capacity, and security to withstand physical harm, severe loads, and other stresses.

The Commission asks whether it should consider independent third-party sources of outage information that might obviate the need to obtain the information directly from broadband ISPs. NCTA is aware of various third party entities that regularly monitor the performance and vulnerabilities of broadband communications, which are confronted with increasingly sophisticated cyber attacks, including botnets, malware, and spyware. We believe that this is another option that should be explored in lieu of regulation.¹⁴

Finally, as the Commission recognized in the *Part 4 Order*, outage data contains highly sensitive information which should be accorded confidential treatment under the Freedom of Information Act (“FOIA”).¹⁵ The Commission recognized that “the disclosure of outage reporting information to the public could present an unacceptable risk of more effective terrorist

¹⁴ See, e.g., Arbor Networks, *ATLAS, About* (“Arbor collectively analyzes the data traversing disparate “darknets” to develop a truly globally scoped view into malicious traffic traversing the backbone networks that form the Internet’s core. With this vantage point, Arbor is uniquely positioned to deliver enterprise and service provider-specific intelligence about malware, exploits, phishing and botnets beyond that being delivered by any other entity today. ATLAS delivers an unprecedented view into Internet scale activity and the ability to discern what new attacks are on the horizon.”), at <http://atlas.arbor.net/about/> (last visited July 7, 2010).

¹⁵ *Part 4 Order*, 19 FCC Rcd at 16834, ¶ 3.

activity.”¹⁶ The competitive and security concerns associated with putting such information in the public record have only intensified since the last time the Commission visited this issue. Any expansion of outage reporting should, therefore, ensure that the data will be protected from public disclosure.

CONCLUSION

In light of the foregoing, NCTA believes that if the Commission moves forward with a comprehensive review of outage reporting in the context of VoIP and broadband communications services, it should proceed through a Notice of Inquiry.

Respectfully submitted,

/s/ Neal M. Goldberg

Neal M. Goldberg
Loretta P. Polk
Steven F. Morris
Jennifer K. McKee
Counsel for the National Cable &
Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

August 2, 2010

¹⁶ *Id.*