

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

In the Matter of	)	
	)	
Public Safety and Homeland Security	)	ET Docket No. 04-35
Bureau Seeks Comment on Whether the	)	WC Docket No. 05-271
Commission's Rules Concerning	)	GN Docket Nos. 09-47, 09-51, 09-137
Disruptions to Communications Should	)	
Apply to Broadband Internet Service	)	
Providers and Interconnected Voice Over	)	
Internet Protocol Service Providers	)	

**COMMENTS OF VERIZON AND VERIZON WIRELESS**

Michael E. Glover  
*Of Counsel*

Karen Zacharia  
Mark J. Montano  
VERIZON  
1320 North Courthouse Road  
9th Floor  
Arlington, VA 22201  
(703) 351-3158

John T. Scott, III  
VERIZON WIRELESS  
1300 I Street, N.W.  
Suite 400 West  
Washington, DC 20005  
(202) 589-3740

Attorneys for Verizon  
and Verizon Wireless

August 2, 2010

**TABLE OF CONTENTS**

INTRODUCTION ..... 1

I. Verizon Already Invests in Features for Its Broadband Networks That Enhance Availability. .... 3

II. Due to the Differences in the Networks, Outage Reporting Rules for PSTN Voice Networks Should Not Be Extended to Broadband Networks. .... 6

III. Other Avenues Exist for the Commission To Obtain Information on Broadband Reliability..... 9

CONCLUSION..... 12

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

In the Matter of	)	
	)	
Public Safety and Homeland Security	)	ET Docket No. 04-35
Bureau Seeks Comment on Whether the	)	WC Docket No. 05-271
Commission’s Rules Concerning	)	GN Docket Nos. 09-47, 09-51, 09-137
Disruptions to Communications Should	)	
Apply to Broadband Internet Service	)	
Providers and Interconnected Voice Over	)	
Internet Protocol Service Providers	)	

**COMMENTS OF VERIZON AND VERIZON WIRELESS**

**INTRODUCTION**

Verizon and Verizon Wireless (“Verizon”) have long taken steps to ensure the availability and reliability of their services. To survive in the highly competitive marketplace, Verizon and other communications providers must be able to offer services that are available when customers wish to access them – even during disasters, severe overloads, cyber attacks, cable cuts, equipment failures, or other unforeseeable events that threaten to disrupt communications. Verizon spends billions of dollars each year – recently estimated around \$17 billion – to build, maintain, and protect the health of its networks.<sup>1</sup> As Verizon’s CEO Ivan Seidenberg explained, “Our job is to make certain those networks are safe and reliable enough for the security of our nation – and our world – to depend on.”<sup>2</sup>

---

<sup>1</sup> See Ivan Seidenberg, Defense Information Systems Agency (DISA) Customer Partnership Conference Keynote Address, [http://www22.verizon.com/Content/ExecutiveCenter/Ivan\\_Seidenberg/defense\\_information\\_systems/](http://www22.verizon.com/Content/ExecutiveCenter/Ivan_Seidenberg/defense_information_systems/) (last visited July 23, 2010).

<sup>2</sup> *Id.*

As described in these comments, Verizon’s broadband networks have a high degree of redundancy and other protective measures in place to keep the networks up or to quickly restore them. Thus, providers like Verizon have taken and are already actively pursuing measures to achieve the very goals the Bureau articulated for requiring broadband outage reports: to “help prevent future outages and ensure a better response to actual outages.”<sup>3</sup>

Moreover, given the significant differences between PSTN voice and broadband networks, the existing outage reporting model is a poor fit for broadband networks. Broadband networks are newer and thus should be even more dependable than today’s highly reliable PSTN voice networks. And due to the broadband networks’ redundancy, lengthy service outages – or even severe congestion – affecting large numbers of Verizon’s broadband customers are relatively rare. Furthermore, requiring *only* broadband providers to report network outages would fail to capture other pertinent information that impedes consumers’ Internet experiences and communications, such as problems with consumers’ equipment or outages in the facilities used by third-parties to provide Internet-based content, applications, and services.

Rather than requiring broadband providers to invest in a reporting system and enforcing such requirements with forfeitures – and thus diverting providers’ resources from responding to outages or adding further protective measures to their broadband networks – the Commission should explore other potential sources of broadband availability and reliability data, including other government and private entities that collect that information today.<sup>4</sup>

---

<sup>3</sup> *Public Safety and Homeland Security Bureau Seeks Comment on Whether the Commission’s Rules Concerning Disruptions to Communications Should Apply to Broadband Internet Service Providers and Interconnected Voice Over Internet Protocol Service Providers*, Public Notice, ET Docket No. 04-35; WC Docket No. 05-271; GN Docket Nos. 09-47, 09-51, 09-137; DA 10-1245, at 2 (July 2, 2010) (“*IP-Outage Notice*”).

<sup>4</sup> Accordingly, Verizon will not address in these Comments whether the Commission would have jurisdiction to require broadband providers to report outages.

## DISCUSSION

### **I. Verizon Already Invests in Features for Its Broadband Networks That Enhance Availability.**

Throughout its history of providing communications services, Verizon has constructed its network knowing that it was important that the network continue to function despite the existence of disasters or other events that could potentially disrupt service. Verizon well understands the need for customers to have communications available and acts promptly to restore service in the event of an outage. Drawing from this experience as a provider of reliable voice services, Verizon deployed its broadband networks to minimize the risks that the network would not be available. Verizon's extensive experience, ranging from local storms to the terrorist attacks of 9/11, has enabled it to hone its processes and safeguards to better withstand future events, whether large-scale disasters or more localized incidents. The key processes and safeguards that Verizon employs are discussed below.<sup>5</sup>

First, Verizon sets an internal goal for the availability of its wireline and wireless broadband networks that is similar to its goal for its voice networks. That is, Verizon endeavors to maintain greater than 99% availability for its broadband network infrastructure, even for its low priced, "best efforts" broadband services. Verizon tracks its performance against its internal goals and makes changes in the networks, including purchasing new equipment and augmenting network capacity, to handle increased consumer demand for bandwidth where required. With respect to its wireless broadband networks, Verizon closely tracks the same metrics for capacity and throughput as well as specific metrics for failed connection attempts and lost connections.

---

<sup>5</sup> The descriptions are at a relatively high level to avoid providing wrongdoers with a roadmap that would allow them to circumvent Verizon's protective measures.

Second, Verizon's broadband networks are designed with a degree of redundancy. Verizon's wireline network is designed to be redundant all the way until the "last mile" to the customer premises. Specifically, for its residential broadband networks, Verizon employs dual-path redundancy from the Internet backbone through the LATA core router to the gateway router. Verizon utilizes two circuits in diverse pathways and houses the LATA core routers in physically separate buildings. Each of the dual paths can carry 100% of anticipated network traffic and is designed to automatically switch over in the event that one of the paths fails. Thus, Verizon's 100% redundant network architecture is able to absorb a large shift in demand for bandwidth due to unforecasted events.

Moreover, even when both paths are available, Verizon's Network Operations Centers (NOCs) closely and proactively monitor traffic for early indications of congestion. Should traffic reach the internal relief threshold, Verizon will augment the path with additional capacity. Verizon also has processes to ensure that facilities are being optimally utilized and to relieve potential overloads in any one given path. Finally, with respect to enterprise and government broadband customers, Verizon supports a range of services, including back-up circuits, diverse entrance facilities at the customer premise, and physically diverse routing options, to ensure that such customers can purchase diverse circuits to meet their needs.

Verizon's wireless broadband network also has redundant assets to help ensure its availability to customers. As with its wireline network, Verizon employs dual path redundancy from the Internet backbone to the mobile switching centers. Furthermore, Verizon's cell sites in urban areas are overlapping. That is, if one site goes down, neighboring sites have capacity in place to handle the downed site's traffic. When necessary, Verizon can augment that capacity.

Verizon has mobile assets, such as Cell On Wheels (COW) and Cell On Light Truck (COLT), that it can deploy when additional capacity is required.

The benefits of Verizon's network redundancy and its efforts to manage capacity were illustrated by the record-breaking snowstorms along the East Coast during February 2010. The snowstorms caused residential utilization peaks to shift from evenings to daytime hours because many people worked from home. Verizon effectively managed this shift, and Verizon's wireline broadband consumers were largely unaffected if they retained electric power. The snowstorms did not result in widespread unavailability or systemic congestion. Similarly, while Verizon observed heavy wireless use in suburban neighborhoods, the snowstorms had little effect on Verizon's wireless networks.

Likewise, President Obama's Inauguration did not adversely affect Verizon's wireless networks despite increases in traffic levels of 100-200%. Verizon moved assets into place ahead of time to handle the expected traffic load. And on that morning, Verizon carefully monitored traffic in real-time and tuned the network by adjusting the footprint of neighboring cell sites to pick up traffic from sites with surges of use. As a result, Verizon experienced a normal day's performance metrics on Inauguration day.

Third, Verizon employs internal physical security practices, including fences, access control systems, alarms, and video surveillance, to guard its critical wireline and wireless network infrastructure. As with other components of the network, the standards to protect Verizon's voice network were used to help develop physical safeguards employed for Verizon's wireline broadband network (which are often located in shared facilities). Buildings are constructed to mitigate risks of natural disasters that are pertinent to the areas in which the buildings are located (e.g., floods, earthquakes, hurricanes, etc.). Moreover, Verizon typically

maintains battery back-up in local backbone sites (e.g., central offices) and in Internet backbone sites. In these sites, Verizon also employs fully independent back-up generator systems. In the wireless network, Verizon's mobile switching centers and the vast majority of its cell sites have alternate power supplies via battery backup and generators.

In sum, all these features work together to enhance Verizon's broadband consumers' ability to access the Internet at any time they want. Such access is a necessity for Verizon to participate in the broadband Internet marketplace, which is highly competitive and becoming more so every day. Verizon, like other broadband providers, already has a substantial incentive to keep its networks up or to quickly restore them and is actively taking steps to do so. As a result, Verizon is presently advancing the Bureau's purported outage reporting goals of "help[ing] prevent future outages and ensur[ing] a better response to actual outages."<sup>6</sup>

## **II. Due to the Differences in the Networks, Outage Reporting Rules for PSTN Voice Networks Should Not Be Extended to Broadband Networks.**

There are significant differences between voice and broadband services that call for the Commission to take a different approach from its rules requiring outage reports for PSTN voice networks should it seek a better understanding of the availability and reliability of broadband networks.

For example, while Verizon's model for its PSTN voice network has been providing service for over 100 years with many network elements in the legacy network being 30 or more years old, Verizon's advanced broadband networks were generally constructed within the past 10-15 years. As a result, Verizon has adopted the best systems and processes from its reliable voice network, including those that may have been learned through trial-and-error. Thus,

---

<sup>6</sup> *IP-Outage Notice* at 2.

Verizon's broadband equipment is newer, self healing, and engineered for redundancy and generally less likely to fail.

In addition, due to the extensive redundancy described in Section I and because broadband networks are more distributed than traditional legacy networks, outages in Verizon's broadband networks tend to affect far fewer customers than outages in the voice network. While outages may occur when a problem exists in the "last mile" of Verizon's wireline broadband network, such outages would impact no more than 1,000 to 2,000 of the millions of customers served, with a majority of these events normally affecting even fewer customers. By comparison, on the PSTN voice network, a single switch outage could affect tens of thousands of customers.

Finally, unlike for voice services, the availability of the broadband service is but one of many factors that impact a consumer's broadband experience. The technology customers use to communicate via a PSTN call is relatively straightforward: two telephones, one for the calling party and one for the called party. The communication can proceed as long as dial tone exists and the connection is maintained.

By contrast, a consumer's broadband experience could be adversely affected by a variety of technological issues that are wholly unrelated to the broadband network. For instance, a consumer may experience a problem with the technology at his or her premise. There could be an issue with the functionality of the home router, whether wired or WiFi, or there could be hardware or software problems on the PC, such as a malfunctioning wireless card or a virus. These problems could slow the consumer's broadband traffic or even impede the consumer's ability to connect to the Internet.

Moreover, the content or application provider that maintains the particular website the consumer seeks to access may be experiencing problems of its own. A fully functioning broadband network does the consumer little good if he cannot reach the sites he wants. Email, for example, continues to be a popular application through which consumers communicate with others via broadband, and consumers depend on their email sites to be working. The media and the sites themselves have sometimes publicly reported significant email outages, including the string of outages in 2008-09 suffered by Gmail,<sup>7</sup> which reportedly has over 170 million users.<sup>8</sup> Website outages, however, are not limited to email. Outages in Apple's MobileMe calendar and contacts applications and Amazon's S3 storage service, upon which many other web applications rely, have been reported in the media.<sup>9</sup> As cloud computing increases in popularity, more and more consumers will be affected by outages at content and application providers' sites.

Indeed, customer reports to Verizon's support centers demonstrate the extent of these customer-impacting issues that are completely unrelated to the availability of the broadband network. Over the past 12 weeks, less than 3% of the customer reports to Verizon's FiOS support centers that customers could not connect to the Internet were due to outages on Verizon's broadband network. The vast majority of such reports were caused by other issues, such as failures in customer premises equipment, spyware, wireless signal strength, and PC network configuration.

---

<sup>7</sup> See [http://www.pcworld.com/article/160153/gmail\\_outage\\_marks\\_sixth\\_downtime\\_in\\_eight\\_months.html](http://www.pcworld.com/article/160153/gmail_outage_marks_sixth_downtime_in_eight_months.html) (chronicling six significant outages of Gmail since July 2008); <http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html> (explaining the cause of the September 1, 2009 Gmail outage) (last visited August 2, 2010)..

<sup>8</sup> See [www.guardian.co.uk/technology/blog/2010/jun/28/microsoft-frank-shaw-numbers-analysed](http://www.guardian.co.uk/technology/blog/2010/jun/28/microsoft-frank-shaw-numbers-analysed) (reporting 173 million Gmail users) (last visited August 2, 2010).

<sup>9</sup> See Rob Pegoraro, *Online Outages, Outrage and Ordeals*, The Washington Post, May 24, 2009.

But the Commission has no visibility into these communication-disrupting outages beyond the media reports or content provider announcements. It follows that requiring *only* providers of broadband networks to file outage reports – but receiving no such information from content and application providers or hardware manufacturers – would give the Commission an incomplete and insufficient view into the Internet user experience.

### **III. Other Avenues Exist for the Commission To Obtain Information on Broadband Reliability.**

Verizon, like many other communications companies, has a close working relationship with the federal agencies and governmental bodies that monitor broadband networks. For example, the National Coordinating Center for Telecommunications (NCC), a part of the National Communications System (NCS), facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications structure, including broadband networks. Verizon has an employee on-site with NCC to enhance Verizon's ability to share relevant status information about its networks should a catastrophic event occur.

In addition, Verizon is engaged with the Communications Sector Coordinating Council (CSCC), which works to protect the United States' communications critical infrastructure and key resources from harm and to ensure that the communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. The CSCC coordinates with the other 17 critical infrastructure sectors through the Partnership for Critical Infrastructure Security (PCIS) to address cross-sector issues and interdependencies. The PCIS provides senior-level cross-sector strategy coordination through partnership with the Department of Homeland Security and the sector-specific federal agencies or SSAs.

In light of the already-established government resources devoted to understanding the availability of broadband networks, the Commission should work with these government bodies to obtain information directly from them during disasters and other large-scale events. With respect to outages of a smaller scale, there are other resources from which the Commission can obtain data to further its understanding of these outages.

For instance, QuEST Forum, an association comprised of global communications service providers and suppliers, developed a quality management system for the communications industry known as TL 9000.<sup>10</sup> TL 9000 specifies measurements for companies to help evaluate the effectiveness of quality implementation and improvement programs and requires the reporting of quality measurement data to a central repository.<sup>11</sup> Such quality measures include customer outages.<sup>12</sup> On a periodic basis, aggregate data, both provider-specific and industry-wide, are reported.<sup>13</sup> Verizon and other broadband providers participate in this association.

Obtaining pertinent data regarding availability through these alternative avenues would benefit both consumers and providers. Consumers would potentially encounter shorter outages as providers could focus their efforts and resources on fixing the conditions that caused an outage, rather than worrying about making accurate, complete, and timely filings within specified windows. Moreover, broadband providers' resources could be used to add further protective measures to their networks – or even to further deploy broadband. And providers may share pertinent data more freely with a private party that would only report anonymized, aggregated data and not hold the threat of enforcement actions and forfeitures over them.

---

<sup>10</sup> See <http://tl9000.org/index.html>.

<sup>11</sup> *Id.*

<sup>12</sup> See <http://tl9000.org/sots/process.html>.

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

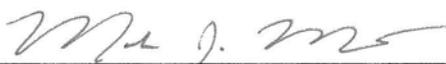
Finally, in addition to gathering data about the availability of broadband networks, the Commission has a role to play in ensuring that broadband customers take appropriate steps to enhance their ability to communicate in the event of network congestion or outage. For example, there are a wide range of activities that end users can undertake to prepare for and help mitigate the effect of a network-affecting event, ranging from limiting broadband use to off-peak time periods to obtaining information from alternative sources, such as broadcast television or radio. In the enterprise space, businesses, too, should take steps to establish alternative means of communications; purchase diverse services for mission critical sites or applications; consider maintaining duplicate “hot sites” from which key data and applications can be accessed in the event of an outage at the primary site; and other such measures.

## CONCLUSION

To meet its customers' expectations in the highly competitive marketplace, Verizon has engineered its broadband networks to be available or promptly restored in the event of an outage. The Commission should not extend its current outage reporting rules to broadband networks due to both the vast differences between PSTN and broadband networks and the availability of information from other sources.

Respectfully submitted,

Michael E. Glover  
*Of Counsel*

  
\_\_\_\_\_  
Karen Zacharia  
Mark J. Montano  
VERIZON  
1320 North Courthouse Road  
9th Floor  
Arlington, VA 22201  
(703) 351-3158

John T. Scott, III  
VERIZON WIRELESS  
1300 I Street, N.W.  
Suite 400 West  
Washington, DC 20005  
(202) 589-3740

Attorneys for Verizon  
and Verizon Wireless

August 2, 2010