

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

In re

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

**REPLY COMMENTS OF SPRINT NEXTEL**

Sprint Nextel Corporation (“Sprint”), pursuant to Public Notice DA 10-1245 issued July 2, 2010 by the FCC’s Public Safety and Homeland Security Bureau (“Bureau”) hereby submits its reply comments in the above-captioned matter. Sprint agrees with those commenting parties that have urged the FCC to proceed with caution, if at all, before subjecting broadband Internet Service Providers (ISPs) and interconnected Voice Over Internet Protocol (“VoIP”) service providers to regulation based on the FCC’s Title II and Title III authority over common carriers and designed for common carrier services providing over the public switched telephone network.

The Bureau is clearly correct that “[c]ommunications services delivered to end users over broadband technologies have grown in importance and now carry some of our most vital communications.” Public Notice at 1. But that fact alone does not necessarily mean that the FCC should expand its Part 4 outage reporting rules to cover broadband ISPs and interconnected VoIP service providers.<sup>1</sup> As nearly all of the parties that submitted comments in response to the

---

<sup>1</sup> The Bureau appears to recognize that the FCC may not have the authority under the Communications Act to prescribe an outage reporting scheme for broadband ISPs and

Public Notice have explained, there is no evidence that even so much as calls into doubt the reliability and resiliency of broadband networks. To the contrary, “the industry has designed and implemented reliable and robust [broadband] networks” and broadband providers “are constantly updating security, reliability and survivability technologies to protect their networks and end user communications.” Comments of the Alliance for Telecommunications Industry Solutions (“ATIS”) at 3. *See also* Comments of the National Cable & Telecommunications Association (“NCTA”) at 2 (“...the complex network infrastructure required to support the diverse needs of broadband communications...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.”); Comments of the United States Telecom Association (USTelecom) at 1 (“Broadband network providers have demonstrated a strong commitment to supporting a highly reliable critical infrastructure capable of providing consumers with services in times of national emergency, local disaster and public health crises”).

The commenting parties also make clear that these highly reliable and resilient broadband networks are not the product of a government mandate. Rather, the demands of a competitive

---

interconnected VOIP providers. Public Notice at 4 (asking for comments on the “strongest sources of authority” for imposing such regulation). Indeed, the FCC has instituted a proceeding in GN Docket No. 10-127 examining the “legal framework of broadband Internet service.” *In the Matter of Framework for Broadband Internet Service, Notice of Inquiry*, released June 17, 2010 at ¶ 2. Moreover, in its proceeding in WC Docket 04-36 (*IP-Enabled and E911 Requirements for IP-Enabled Service Providers*), the FCC is still considering the question of how to classify interconnected VoIP providers under the Communications Act, although such providers are currently subject to various requirements based on the FCC’s authority under Title II of the Act. Thus, any action in this matter may have to – and perhaps should – await the outcomes of these two proceedings.

marketplace require broadband ISPs and interconnected VoIP service providers to offer a highly reliable service. Comments of Qwest Communications International, Inc. (“Qwest”) at 6-7; Comments of AT&T, Inc. (“AT&T”) at 6; Comments of MetroPCS Communications, Inc (“MetroPCS”) at 4-6; Comments of USTelecom at 3; Comments of ATIS at 3-4.

Yet another factor weighing against the imposition of outage reporting requirements on broadband ISPs and interconnected VoIP service providers is the complexities of the networks necessary to furnish IP-enabled broadband services to end users. Indeed, it is highly problematic that the providers of such services would be able to determine the cause of many, if not all, disruptions in service as perceived by end users let alone its severity. An end user, for example, may be unable to reach his desired Internet destination not because of a problem with his chosen ISP or the Internet backbone network used by the ISP to transport the end user’s communications but because of problems with the user’s computer, *e.g.*, a virus or other form of malware, or because the Internet destination cannot readily accept the traffic due to a congestion being generated by a denial-of-service attacks by criminals or individuals or groups of individuals working on behalf of foreign governments.<sup>2</sup> *See* Comments of the United States Internet Service Provider Association at 2; Comments of MetroPCS at 6; and Comments of ATIS at 4.

---

<sup>2</sup> It is well-recognized that one of the major problems in ensuring that America’s critical cyber infrastructure is secure is that end users (both residential and small to medium-sized businesses) are unaware of the need to protect their computers from those seeking to implant a virus or other form of malware so as to steal any personal information stored on the computer or otherwise control the computer as part of a so-called bot network. In fact, a key part of President Obama’s plan to make America’s digital infrastructure is to raise the public’s cybersecurity awareness and the need to take steps install (and update) software designed to counter, if not totally prevent, the malicious acts of criminals and other evil doers. *See* the President’s Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (White House 2009) and the Comprehensive National Cybersecurity Initiative. *See* <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

In all events, Sprint believes that the costs that would have to be expended by broadband ISPs and interconnected VoIP service to develop a system for reporting outages outweigh whatever putative benefits the FCC assumes it would gain by having such information, especially since the reports themselves would unlikely produce any useful data. Moreover, absent FCC decisions in GN Docket No. 10-127 and WC Docket 04-36, the imposition of such a reporting scheme may be of questionable legality. *See* footnote 1 *supra*. Thus, Sprint, like most of the parties that submitted comments in response to the Public Notice, recommends that the FCC not issue a Notice of Proposed Rulemaking (“NPRM”) looking toward subjecting broadband ISPs or interconnected VoIP service providers to outage reporting.

Sprint recognizes, of course, that the FCC may not agree with Sprint’s recommendation here. If so, Sprint believes that any proposed FCC reporting scheme will have to be based on the specific characteristics of Internet broadband and interconnected VoIP services. Indeed, if anything, the record in this proceeding confirms that the FCC “should not simply shoehorn VoIP and broadband Internet services into [the] existing outage reporting standards” prescribed in Part 4 of the FCC’s Rules. Comments of NCTA at 7. Various parties have put forth the standards upon which such reporting system, at a minimum, should be based. For example, the triggering mechanism for submitting an outage report must be based on objective criteria as opposed to the vague notion of end user perceptions, *see e.g.*, Comments of CTIA – The Wireless Association (“CTIA”) at 5-6. Broadband ISPs and interconnected VoIP providers should only have to report outages that occur on the facilities they own or control and not outages on the facilities of others

---

Sprint has recommended that the FCC participate in this educational initiative by launching a cybersecurity public awareness campaign to provide consumers with the necessary information on how to protect themselves from cyber threats. *See* July 12, 2010 Comments of Sprint in PS Docket 10-93 (In the Matter of Cyber Security Certification Program) at 11-12.

entities that may be involved in the provision of their services, Comments of AT&T at 8. And the reporting deadlines must be realistic, *see e.g.*, Comments of AT&T at 9; Comments of Qwest at 12.

Of equal, if not greater importance, all reports submitted by broadband ISPs and interconnected VoIP service providers must be kept confidential. In this regard, the California Public Utilities Commission (“CPUC”) the District of Columbia Public Service Commission (“DCPSC”) and the New York State Public Service Commission (“NYPSC”) argue that they should receive whatever reports are filed by broadband ISPs and interconnected VoIP service providers detailing outages that impact their residents. *See* Comments of the CPUC at 3; Comments of the DCPSC at 3; Comments of the NYPSC at 1. All three commissions appear to recognize the need to ensure the confidentiality of any of the outage reports they receive. Comments of the CPUC at 9; Comments of the DCPSC at 3; Comments of the NYPSC at 3. Nonetheless, as CTIA points out, “[s]haring data with additional parties geometrically increases the risk of disclosure and makes it more difficult to identify the source of breaches.” Comments of CTIA at 7. *See also* Comments of Qwest at 12-14; Comments of ATIS at 8; Comments of NCTA at 12-13. Thus, before the FCC determines to allow access by a state agency to any outage reports submitted by the broadband ISPs and interconnected VoIP service providers despite the fact that the States do not have jurisdiction over the provision of such services and could not use the reports to impose state specific requirements on such providers, the FCC must ensure that such state’s sunshine or public access laws would not risk the disclosure of

these confidential reports. Comments at CTIA at 7 and Comments of Qwest at 14.

Respectfully submitted,

SPRINT NEXTEL CORPORATION

A handwritten signature in black ink, appearing to read "Michael B. Fingerhut", is written over a horizontal line. The signature is fluid and cursive.

Charles W. McKee  
Michael B. Fingerhut  
900 7<sup>th</sup> Street NW Suite 700  
Washington, DC 20001  
(703) 592-5112  
Its Attorneys