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

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	WC Docket No. 11-39
The Truth in Caller ID Act of 2009	)	

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net Coalition ("VON")[1] hereby submits these comments in response to the Notice of Proposed Rulemaking issued in the above-referenced proceeding.[2] In this proceeding, and pursuant to the congressional mandate contained in the Truth in Caller ID Act of 2009 (the "Act")[3], the Commission must issue implementing regulations within six months of the law's enactment.[4] The *NPRM* details the proposed rule implementing the Act and also seeks comment on numerous issues including, but not limited to, whether: (1) the proposed rule fulfills Congress' intent; (2) to include "knowingly" in the standard when determining whether a violation of the rule has occurred; and (3) the existing definition of interconnected voice over Internet protocol service should be superseded by the Department of Justice's definition of IP-Enabled Voice Service.

---

[1] The VON Coalition works to advance regulatory policies that enable Americans to take advantage of the promise and potential of IP-enabled communications. VON Coalition members include AT&T, Broadvox, BT, Google, iBasis, Microsoft, Skype, T-Mobile, Vonage and Yahoo.

[2] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Notice of Proposed Rulemaking, 26 FCC Rcd 4128 (2011) ("*NPRM*").

[3] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

[4] *Id.* § 227(e)(3). President Obama signed the Act into law on December 22, 2010.

INTRODUCTION

Thanks to innovation, voice communications have transitioned from wireline to wireless in a matter of 100 years and from wireless to voice over Internet protocol ("VoIP") in a matter of 20 years.[5] Innovation does not deter bad actors. As with any product, service, application, or technology, the potential that someone can use an innovative and generally beneficial technology in harmful or dangerous ways is present. Users of new voice applications and services have more control over the outgoing content of information provided to the public, including the ability to customize or conceal their true identities and telephone numbers. Unfortunately, Caller ID can be susceptible to misuse and abuse by some individuals,[6] who, through the employment of specific devices[7] or with the assistance of certain third party caller ID spoofing providers,[8] seek to deceive, defraud, and/or harm the public.

To thwart abuses, Congress has enacted laws focused on protecting consumers' interests and privacy. The Act serves to protect the public against individuals and entities who, using spoofing capabilities, are intent on perpetrating fraud and malicious behavior against members of the public and public safety organizations.[9]

---

[5] http://en.wikipedia.org/wiki/History_of_mobile_phones (retrieved Apr. 13, 2011).

[6] The ability to spoof caller ID is not limited to VoIP services. Individuals have been spoofing caller ID since caller ID was first made publicly available. *See, e.g.*, http://www.artofhacking.com/files/OB-FAQ.HTM

[7] For instance, an Orange Box is a device that can emulate the Caller ID signal that is transmitted to a telephone line from its Central Office following the beep of an incoming Call Waiting call. *See* http://www.artofhacking.com/files/OB-FAQ.HTM (retrieved April 18, 2011).

[8] *NPRM* at ¶ 21. Spoofing is the "deliberate falsification of the caller ID number in order to disguise the identity and originator of the call." http://www.fcc.gov/cgb/consumerfacts/callerid.html (retrieved Apr. 13, 2011).

[9] *NPRM* at ¶ 1. Callers, tricked by spoofed caller ID information, have been coerced into providing their social security numbers after being threatened with criminal prosecution for failure to appear for jury duty. Additionally, callers, employing spoofing services, have engaged in the practice referred to "swatting," which involves placing false emergency calls to law enforcement agencies to elicit a response from Special Weapons and Tactics (SWAT) teams. *Id.* at ¶ 8.

I. The Commission's Proposed Rule Fulfills Congress' Intent to Stop Deceit, Fraud and Mayhem by Individuals and Fraudulent Spoofing Services

The VON Coalition supports the Commission's proposed rule, which expands the Act's compliance obligations from individuals to individuals *and* entities alike; requires actual knowledge of intent to defraud, harm, or wrongfully obtain anything of value; accommodates instances of legitimate manipulation of caller identification information;[10] and recognizes the real-world provision of communications services and applications to consumers across numerous and unrelated providers and platforms.

The Act "makes it unlawful for any person, in connection with any real-time voice telecommunications service, regardless of technology, to cause any caller identification service to transmit misleading or inaccurate caller ID information with the intent to defraud or deceive."[11] The Act, as written, appears to limit culpability to individuals alone. Moreover, the Act's phrase "to cause any caller identification service to transmit" might be construed inaccurately by some to impose third party liability on the unknowing service or application provider who is merely a conduit in the delivery of the information. In the context of the real-world provision of services, multiple service or application providers may be involved with the delivery of a single voice communication. The Commission resolves the legislative intent by expanding compliance obligations beyond individuals to both individuals and entities. This achieves Congress' underlying goal – to stop malicious, fraudulent and harmful actions of the

[10] Both Congress and the Commission provide examples whereby manipulation of caller ID information is acceptable, including voice communications from domestic violence shelters, call blocking options, and PBX centers. *Id.* at ¶ 7.

[11] *See* 47 U.S.C. § 227(e)(1) (stating that "[i]t shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted...").

Caller ID spoofer, not to retard VoIP innovations or impose liability on the provider of the transmission conduit who does not have advance knowledge.

II. Knowledge of Intent to Defraud, Cause Harm, or Wrongfully Obtain Anything of Value Must be Borne by Callers and Spoofing Services Alike For a Violation of the Rules To Occur

Under the proposed rule, responsibility for violations must be shared by individuals having the requisite knowledge that manipulate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value and/or the third party spoofing service that provides the means by which to manipulate such information.[12] To avoid penalizing service and application providers for the unknown provision of inaccurate or misleading caller ID information and stymieing innovation, the proposed rule requires that individuals and entities (i.e., service providers and third party spoofing services) have advance knowledge of the intent to defraud, harm, or wrongfully acquire anything of value. The advance knowledge of such intent on the part of the application or service provider must be present for a violation of the rule to occur.

The requirement that knowledge must be present effectively and rightfully exempts traditional caller identification service providers from violations of the rule. The exemption is based on a traditional service provider's pass-through activities and negligible contact with a caller. Consequently, the traditional service provider generally lacks the requisite knowledge that an individual or entity intends to defraud, harm, or wrongfully obtain anything of value from a consumer. As the Commission acknowledges, "in many instances, the caller identification service has no way of knowing whether or not the caller identification information it receives has

[12] *NPRM* at ¶12 and proposed rule 64.1604 found at *NPRM*, Appendix A ("[n]o person or entity in the United States, shall, with the intent to defraud, cause harm, or wrongfully obtain anything of value, ***knowingly*** cause, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information.") (emphasis added).

been manipulated."[13] Accordingly, any individual or entity that *knowingly* facilitates the nefarious use and abuse of caller ID technology – with the requisite intent to defraud or cause harm – would violate the Act and the Commission's rules.[14]

III. IP-Enabled Services Should Reflect the Commission's Definition of Interconnected Voice over Internet Protocol

The *NPRM* also seeks comment on the interchangeability of the definition of "IP-Enabled Services" as contained in the Act and the definition of "interconnected VoIP" in Section 9.3 of the Commission's rules.[15] The Commission should, consistent with the Act, use the established definition of interconnected VoIP, and not the broader definition cited by the Department of Justice.[16] This is not the appropriate proceeding for the Commission to create a new regulatory framework for services previously not subject to regulation.

The Act states, "[i]t shall be unlawful for any person within the United States, in connection with any telecommunications service or *IP-enabled voice service*,…."[17] Subsection (e)(8)(C) indicates that the term IP-enabled voice service has the same meaning as Section 9.3 of the Commission's rules, which among other things, defines interconnected VoIP.[18] The VON Coalition contends that slight variation in descriptive terms does not render the terms "IP-enabled voice service" and "interconnected VoIP" as inconsistent or evidence of Congressional intent to expand liability beyond the codified definition of interconnected VoIP.

The Commission also seeks comment on a proposal by the Department of Justice whether to abandon for this particular proceeding its existing definition of interconnected VoIP and elect

---

[13] *NPRM* at ¶ 13.

[14] Thus, a third party spoofing service would be noncompliant only if it had knowledge of the fraudulent or malicious intent by the individual employing the spoofing services.

[15] *NPRM* at ¶ 15.

[16] *Id.*

[17] 47 U.S.C. § 227(e)(1).

[18] *Id.* § 227(e)(8)(C).

to use the definition of IP-Enabled Voice Services as detailed in Title 18 of the U.S. Code.[19] According to the *NPRM*, the distinction between the statute and the regulation centers on the breadth of the former because the statute would not require "the use of a broadband connection or the ability to originate and terminate traffic from the public switched telephone network."[20] The proposed rule refers to the transmission or display but does not specifically state which service or method of communication must be employed by the individual or entity. In the *NPRM*, the Commission indicates that the "proposed rules define "caller identification service"[21] and "caller identification information"[22] to encompass calls made by using a telecommunications service or interconnected VoIP; therefore, the proposed rules would apply to calls made using either type of service.[23] To retain consistency in the Commission's proceedings, the VON Coalition believes that the terms used in the proposed rule are sufficient to meet Congressional intent. Therefore, the VON Coalition does not support the limited use of an alternative definition of IP-Enabled services.

[19] 18 U.S.C. § 1039(h)(4).

[20] *NPRM* at ¶ 15.

[21] Proposed 47 C.F.R. § 64.1600(d) defines caller identification service as "any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service. Such term includes automatic number identification services."

[22] Proposed 47 C.F.R. § 64.1600(c) defines caller identification information as "information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service."

[23] *NPRM* at ¶¶ 16-17.

CONCLUSION

For the foregoing reasons, the VON Coalition respectfully requests that the Commission act consistently with the recommendations made herein. The VON Coalition also looks forward to working with the Commission in this important proceeding on the implementation of the Act.

Respectfully submitted,

VOICE ON THE NET COALITION

/s/

Glenn S. Richards
Executive Director
2300 N Street NW
Washington D.C. 20037
glenn.richards@pillsburylaw.com
(202) 663-8215

April 18, 2011