FEDERAL COMMUNICATIONS COMMISSION
CHAIRMAN JULIUS GENACHOWSKI

CALLER IDENTIFICATION INFORMATION IN SUCCESSOR OR REPLACEMENT TECHNOLOGIES

Submitted Pursuant to
Public Law No. 111-331

June 22, 2011

Table of Contents

I. INTRODUCTION AND EXECUTIVE SUMMARY

1. This Report is submitted to Congress by the Chairman of the Federal Communications Commission (FCC or Commission),[1] pursuant to the Truth in Caller ID Act of 2009 (Truth in Caller ID Act).[2] The Truth in Caller ID Act prohibits the spoofing of caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[3] Fraudulent and harmful spoofing has become increasingly widespread, with serious economic and public safety consequences. The Truth in Caller ID Act, which was signed into law by President Obama on December 22, 2010, directs the Commission to adopt implementing rules and "report to Congress whether additional legislation is necessary to prohibit the provision of inaccurate caller identification information in technologies that are successor or replacement technologies to telecommunications services or IP-enabled voice service."[4] The Commission issued rules implementing the Truth in Caller ID Act on June 22, 2011.

2. In furtherance of its obligation to adopt rules implementing the Truth in Caller ID Act, the Commission issued a Notice of Proposed Rulemaking on March 9, 2011, seeking comment on proposed rules. To assist in the preparation of this Report, the Commission also sought comment on what "technologies parties anticipate will be successor or replacement technologies to telecommunications services or IP-enabled voice services," and on the "provision of inaccurate caller identification information with respect to such technologies."[5] The Report discusses areas identified by commenters where the statute and the Commission's implementing rules may fall short of protecting consumers from caller identification spoofing done with the intent to defraud, cause harm, or wrongfully obtain anything of value.[6] Looking forward, the Report discusses several newer types of communications services including, for example, text messaging and social media, and identifies issues that may arise with the potential to deceive consumers by providing inaccurate identification information in conjunction with such services.

3. This Report is organized as follows: This Part I provides an introduction to and

---

[1] *See* 47 U.S.C. §155(a) (stating that "[i]t shall be [the Chairman's] duty . . . to represent the Commission in all matters relating to legislation and legislative reports").

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

[3] We use the term "spoofing" in the popular sense of knowingly using identification information to masquerade as a different person or entity.

[4] 47 U.S.C § 227(e)(4). The Truth in Caller ID Act specifies that the term "IP-enabled voice service" has the "meaning given that term by section 9.3 of the Commission's regulations (47 C.F.R. 9.3)." 47 U.S.C. § 227(e)(8)(C). Section 9.3 of the Commission's rules defines "interconnected Voice over Internet Protocol (VoIP) service," not "IP-enabled voice service," and we use the term "interconnected VoIP services" here rather than "IP-enabled voice service" to be consistent with the Commission's existing rules and the direction in the Truth in Caller ID Act. The Commission defines interconnected VoIP as a service that: "(1) Enables real-time, two-way voice communication; (2) Requires a broadband connection from the user's location; (3) Requires Internet protocol-compatible customer premises equipment (CPE); and (4) Permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network." 47 C.F.R. § 9.3.

[5] *See Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, 26 FCC Rcd 4128, 4141, para. 35 (2011) (*Caller ID Act NPRM*).

[6] The Commission received comments and reply comments from 37 stakeholders, including law enforcement agencies, carriers, trade groups, consumer groups, technology companies, and individuals.

executive summary of the Report. Part II reviews the technological evolution of caller identification information manipulation. Part III describes the application of the Commission's rules implementing the Truth in Caller ID Act, and addresses caller identification manipulation using voice call technologies that remain uncovered by the Commission's rules implementing the Truth in Caller ID Act. Part IV examines caller ID aspects of technologies underlying current trends in communications. Finally, Part V provides legislative recommendations to tighten the current prohibitions on malicious caller ID spoofing and to address identification spoofing in new and emerging communication services. Legislative recommendations include clarifying the scope of the Truth in Caller ID Act to include (1) persons outside the United States, (2) the use of IP-enabled voice services that are not covered under the Commission's current definition of interconnected Voice over Internet Protocol (VoIP) service, (3) appropriate authority over third-party spoofing services, and (4) SMS-based text messaging services.

II. BACKGROUND

A. Caller ID Services[7]

4. A Caller ID service permits the recipient of an incoming call to determine the telephone number of the calling party and, in some cases, a name associated with the number before answering the call. Network technologies and interconnection arrangements that have been deployed in recent years to provide new communications services make it easier to manipulate information identifying the caller on an incoming call. The accompanying growth of caller ID manipulation, or spoofing, has brought with it increased concerns about security, privacy, and other consumer harms. Congress took a major step towards addressing malicious caller ID spoofing by enacting the Truth in Caller ID Act of 2009, which prohibits anyone in the United States from knowingly causing any caller identification service to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[8]

5. The history of today's Caller ID service goes back to the early 1980s. Caller ID service became a practical local service offering in that era when local exchange carriers (LECs) began adopting Signaling System No.7 (SS7) signaling techniques to route and manage telephone calls.[9]

---

[7] We use the term "caller identification service" to mean any service or device that meets the statutory definition of being "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 IP-enabled voice service." 47 U.S.C. § 227(e)(8)(B). Caller identification services include "Caller ID services," a term that we use here to refer specifically to services that permit the recipient of an incoming call to determine, before answering, the calling party number and, in some cases, a name associated with the number. Caller identification services is a broader category and includes services other than Caller ID services, such as charge number services and automatic number identification (ANI) services including, for example, those used by public safety answering points.

[8] *See* 47 U.S.C. § 227(e)(1) ("In General.—It 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 pursuant to paragraph (3)(B).").

[9] *See Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Memorandum Opinion and Order on Reconsideration, Second Report and Order and Third Notice of Proposed Rulemaking, 10 FCC Rcd 11700, 11704–05, paras. 7–11 (1995) (*Second Caller ID Order*); *see also Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Notice of Proposed Rulemaking, 6 FCC Rcd 6752, para. 2 (1991) (*Caller ID NPRM*).

As shown in Figure 1, SS7 techniques place digital signaling information on a transmission channel separate from the audio voice communications channel. Audio voice communication traditionally has been transmitted using switched time-division multiplexing (TDM) technology. SS7 signaling enabled providers to represent and transfer the Calling Party Number (CPN) information that is used for Caller ID services across multiple carriers in addition to transmitting and switching the audio voice communication.[10] The CPN information used in SS7 was generally not changeable by the calling party. The CPN information for residential users was mainly under the control of the caller's LEC. Business users with Private Branch Exchange (PBX) facilities often had some ability to change their CPN information, but such changes were usually applied consistently to all outgoing calls rather than varying on a call-by-call basis.

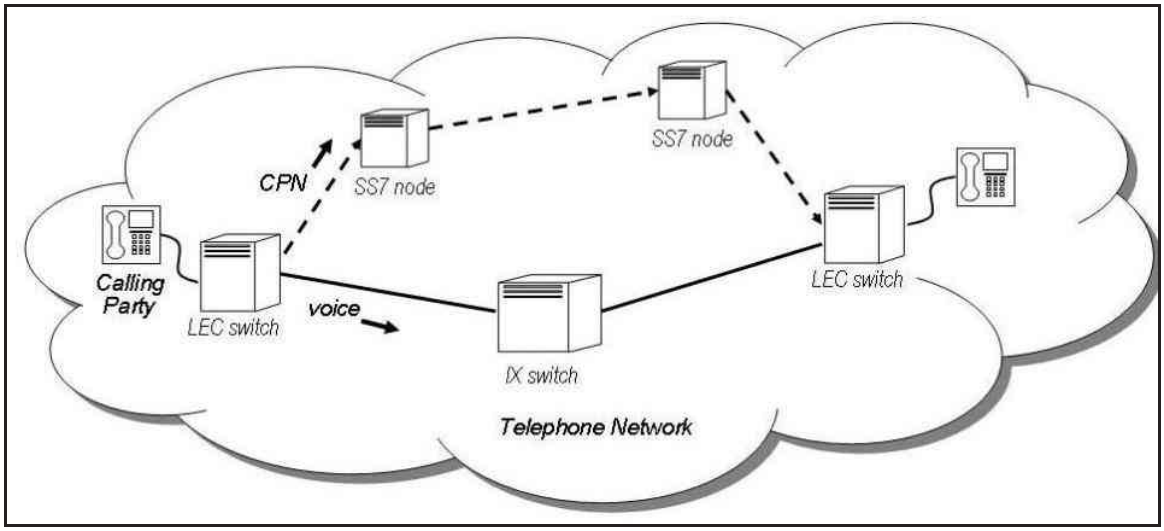

Figure 1. Managing Calling with Signaling System 7

6. In the 1990s, the Commission adopted rules to address interstate Caller ID and other CPN-based services.[11] Under the Commission's rules, common carriers that use SS7 generally must transport the CPN on interstate calls to interconnecting carriers.[12] In addition, a calling party can request that his or her calling number and name be blocked, *i.e.*, not revealed to the called party. This can be done on a touch-tone telephone by pressing *67 before entering the

[10] *See Caller ID NPRM*, 6 FCC Rcd at 6752, paras. 1–2. Early subscribers to Caller ID services typically paid a monthly fee for Caller ID service and usually had to purchase a separate device that received and displayed caller ID information. *Id*. Today, Caller ID service is provided as a standard feature of many telephone services, including mobile phone services.

[11] *See Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 1764 (1994) (*First Caller ID Order*); *Second Caller ID Order*, 10 FCC Rcd 11700.

[12] 47 C.F.R. § 64.1601. In February, 2011, the Commission adopted a notice of proposed rulemaking that proposed, among other things, revising this rule to expand the CPN transport requirement to apply to interconnected VoIP service providers and to intrastate traffic. *See Connect America Fund; A National Broadband Plan for Our Future; Establishing Just and Reasonable Rates for Local Exchange Carriers; High-Cost Universal Service Support; Developing a Unified Intercarrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up*, WC Docket Nos. 10-90, 07-135, 05-337, 03-109, CC Docket Nos. 01-92, 96-45, GN Docket No. 09-51, Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking, 26 FCC Rcd 4554, 4751, para. 620 (2011) (*USF/ICC Transformation NPRM*).

destination phone number.[13] Carriers using SS7 or any service based on SS7 call set-up functionality are required to recognize and honor calling parties' privacy requests. As a result, on a call-by-call basis, most callers have the ability to block a call recipient from seeing the caller's telephone number or name. Whether the CPN and other caller identification information are revealed to the called party generally depends on whether the called party receives Caller ID service from his or her service provider and, if so, whether the calling party has requested privacy.[14] This basic framework reflects the Commission's balancing of the benefits of Caller ID service with the privacy issues raised by this and other CPN services.[15]

7. When the Commission first adopted its rules relating to CPN, Caller ID service was still relatively new. The Commission did not require the adoption of SS7 techniques, although over time most telecommunications carriers in the United States did adopt SS7 and, consequently, Caller ID and other services based on the CPN became commonplace. Because the terminating provider often had no direct relationship with the person placing a call, that terminating provider generally had no way to verify whether the caller identification information it received was accurate. Nevertheless, because the CPN was under the control of the originating LEC or a corporate PBX, and was transmitted using SS7 signaling techniques end-to-end, it was generally considered information that could be trusted by the receiver. As carriers and other entities have begun migrating to Internet Protocol (IP) networks to carry both voice and signaling, however, new signaling techniques have emerged. Interconnected VoIP providers, for example, often use the industry-standard Session Initiation Protocol (SIP) signaling techniques, rather than SS7.[16] These new technologies, in conjunction with other marketplace developments, have lessened the overall accuracy and reliability of caller identification information.

[13] 47 C.F.R. § 64.1601(b).

[14] The Commission's rules exempt certain types of calls, including calls from payphones and from most Private Branch Exchanges, from the requirements to transmit CPN and to recognize and honor calling parties' privacy requests. *See* 47 C.F.R. § 64.1601(d).

[15] The Commission's rules concerning the delivery of CPN also address the transmission and use of Automatic Number Identification (ANI) information, which is information about the caller's phone number used for charging purposes, and may or may not be the same as the CPN. *See* 47 C.F.R. § 64.1602. When the Commission adopted its rules, it found that ANI blocking was not technologically feasible, and that use of ANI did not raise the same privacy concerns as the use of CPN services. Therefore, instead of requiring that ANI blocking be made available to subscribers, the Commission required carriers offering ANI services to limit the permissible uses of ANI. *See First Caller ID Order*, 9 FCC Rcd at 1772–74, paras. 51–58.

[16] *See supra* note 4 for the definition of "interconnected VoIP." *See also* Rosenberg *et al.*, *SIP: Session Initiation Protocol*, Memorandum from the Internet Engineering Task Force on Internet Standards Track Protocol to the Internet Community, RFC3261 (June 2002*)*, *available at* http://www.ietf.org/rfc/rfc3261.txt. Vendor-specific *de facto* standard signaling protocols, such as the Inter Asterisk eXchange protocol, are also widely used for interconnected VoIP signaling. *See, e.g.*, Spencer *et al.*, *IAX: Inter-Asterisk eXchange Version 2*, Memorandum from the Internet Engineering Task Force on the Inter-Asterisk eXchange protocol to the Internet Community, RFC 5456 (Feb. 2010), *available at* http://www.ietf.org/rfc/rfc5456.txt.

B. Interconnected VoIP Services[17]

8. In general, the low cost and widespread availability of VoIP technologies and services have increased the control that calling parties can exercise over the information transmitted with their phone calls. Some interconnected VoIP services, such as those provided by many cable system operators, are designed to work in the same manner for end-user customers as a LEC service; in those cases, the caller is unable to modify the CPN.[18] However, other Internet-based voice services, including many provided as third-party applications used in connection with broadband services,[19] allow the calling party to make a call appear to come from another phone number. For example, users of some Internet-based voice services can specify and validate their mobile phone number as the CPN, allowing them to originate outgoing calls from the Internet to the Public Switched Telephone Network (PSTN) and receive incoming calls over the PSTN to their cell phone.[20] More sophisticated users can download free open-source software to a conventional personal computer that enables that computer to function as an IP-based PBX or a VoIP gateway.[21] The user then can originate calls with spoofed Caller ID information and transfer those calls from the Internet to the PSTN through a VoIP call termination service.[22]

C. Third-Party Spoofing Services

9. Less technologically-sophisticated users of either traditional telephone services or interconnected VoIP services can easily spoof their caller ID by purchasing or otherwise obtaining caller ID spoofing services from third parties. Indeed, such caller ID spoofing services openly advertise their services on the Web, and some sell prepaid cards providing a certain number of minutes of spoofing services through retail stores.[23] These services may offer

---

[17] We use the term "interconnected VoIP services" in place of "IP-enabled voice service" to be consistent with the Commission's existing rules and the direction in the Act. *See supra* note 4.

[18] For example, in a 2006 informational presentation to Commission staff entitled "Digital Phone VoIP-Based Services & Caller ID," Time Warner Cable noted that "Subscribers are unable to modify their own number; Works in the same manner as traditional Class5 switching." Time Warner Cable, Remarks at an Informational Presentation to the Federal Communications Commission Staff (Apr. 25, 2006).

[19] Such services are sometimes referred to as "over-the-top" VoIP.

[20] The validation is done, for example, by sending text messages to the mobile phone number. *See, e.g.*, Skype, *How to Set Up Caller ID. . .*, (2011), http://www.skype.com/intl/en/features/allfeatures/caller-identification/; Google Voice, *Making Calls*, (2011), http://www.google.com/support/voice/bin/answer.py?hl=en&answer=115079. With some VoIP services, if the user doesn't or can't specify a CPN, the provider may insert a meaningless default CPN (or no CPN) which can be a source of confusion to called parties with Caller ID service.

[21] *See* TelTech Comments at 5–7, WC Docket No. 11-39 (filed Apr. 18, 2011).

[22] For purposes of this report, by VoIP termination provider we mean an entity that operates a gateway service between the Internet and the PSTN, and transfers call signaling and voice between the two environments. *See id*. at 6 ("After the customer has made her choices, the Asterisk program re-directs the call back to TelTech's wholesale VOIP termination provider. When the IP call is converted back to TDM for termination, the SS7 Caller ID field is derived from the SIP CPN field."). For an example of VoIP termination service, see Verizon, *VoIP Termination Service*, (2009), http://www22.verizon.com/wholesale/voip/termination/0,5830,3,00.html.

[23] *See, e.g.*, ITELLAS COMMUNICATIONS, *Caller ID Spoofing* (2010), http://www.itellas.com ("Welcome to our caller ID spoofing site!"); TELESPOOF.COM, *Spoof Caller ID With Telespoof.com* (2011), http://www.telespoof.com ("[T]he highest quality caller ID service available anywhere in the world."); PHONEGANGSTER.COM (2011), http://www.phonegangster.com (allowing customers to "fake the caller id

additional options, such as the ability to record the call or even to digitally disguise the caller's voice. Businesses also use third-party services for manipulating CPNs. Some businesses with large call centers, such as telemarketers and debt collectors, employ companies that provide call management services, including the ability to alter caller identification information. Such companies often substitute a number with the same area code as the called party's area code to increase the likelihood that the called party will answer.[24]

10. Figure 2, below, illustrates the popular technique of using a third-party caller ID spoofing service offered to the public to spoof the phone number displayed by the called party's Caller ID service.[25] In the example depicted in Figure 2, the caller has already created an account with a caller ID spoofing service or purchased a prepaid calling card, and has a personal identification number (PIN) he uses to access the spoofing service. In order to make a call with a spoofed caller ID, the caller dials the spoofing service's toll free number and, when connected to the spoofing service, the caller enters his PIN, the telephone number he wants to call, and the number he wants to have displayed by the called party's Caller ID service (the "substitute number"). The spoofing service forwards the call to the telephone number specified by the caller and forwards the "substitute number" as the CPN. As a result, the called party's Caller ID service displays the substitute number as the caller ID.

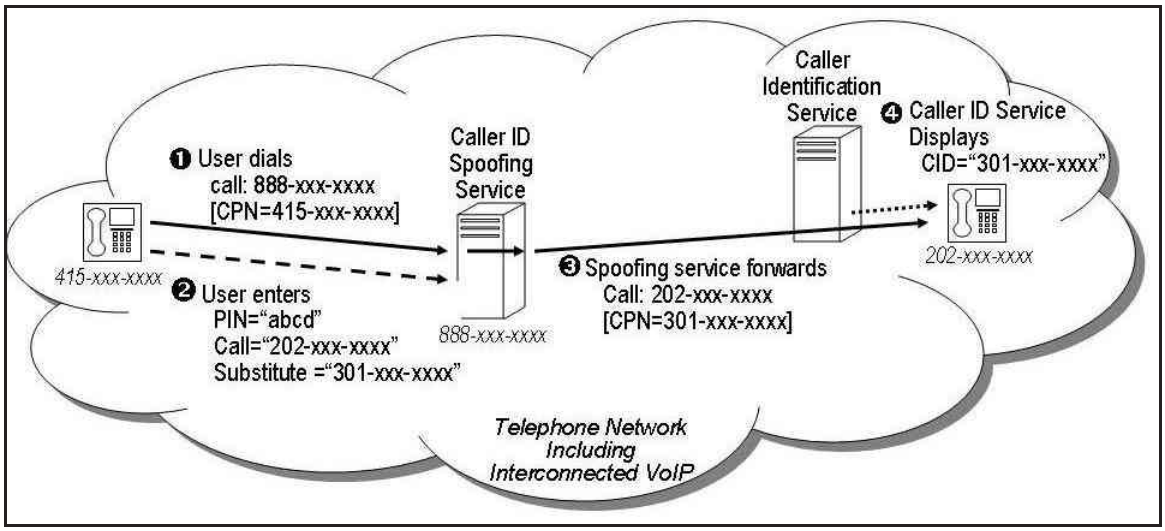

Figure 2. Operation of Third-Party Spoofing Service

when calling another party"); SPOOFAPP (2011), http://www.spoofapp.com ("Disguise your caller ID and be anyone."); SPOOFCARD, http://www.spoofcard.com ("Call someone from your phone and the person's Caller ID displays the number that you intend them to see."); *see also* TelTech Comments at 9 ("TelTech also sells pre-paid cards for the SpoofCard and other services. These cards are sold to wholesalers, who then resell them to retailers for sale in kiosks, grocery stores and other retail outlets.").

[24] *See, e.g.*, NobelBiz Comments at 1, WC Docket No. 11-39 (filed Apr. 18, 2011) ("NobelBiz enables a wide range of businesses to establish a local market presence through the use of local area codes. . . . LocalTouch permits a calling party to make a long distance voice call that is received by the called party as a local call. For businesses that seek to contact individuals by telephone, LocalTouch results in a higher call completion rate.").

[25] There are means other than third-party spoofing services by which caller identification information can be manipulated, but this is the means most accessible to the general public.

11. Some third-party spoofing services may caution against fraudulent or illegal use of their services or take steps to prevent certain types of spoofing. For example, some third-party spoofing services block calls to certain numbers or prevent the user from specifying certain high-profile numbers as the substitute CPN (e.g., the phone number of the White House switchboard).26 In general, however, the operator of the third-party spoofing service is not aware of the intent of a user of the spoofing service or whether the user has any valid right to use the substitute number entered. Often the substitute number will have been assigned to another telephone service customer who has neither authorized nor been made aware of its use as a substitute number. The telephone service customer whose number is used as the substitute number without his knowledge may therefore become the victim of consequences that are at best annoying and at worst significantly costly and harmful. For example, one commenter received 24 subpoenas and experienced overloaded trunks in connection with one of its phone numbers that was substituted as the CPN number that appeared on Caller ID devices on hundreds of thousands of calls.[27]

12. A caller ID spoofing service such as that shown in Figure 2 can be directly connected to the PSTN with a conventional trunk connection that supports multiple voice circuits, in the same manner as a traditional (*i.e.*, non-IP-based) business PBX. However, it is more typical for the spoofing service to be connected to the publicly-accessible Internet only. Calls to and from the service are routed over the Internet between the spoofing service and a VoIP call termination provider that serves as a gateway for transferring calls between the Internet and the PSTN. In this more common, Internet-based spoofing service configuration, a call may come from the TDM-based PSTN, be passed through a VoIP call termination provider gateway and delivered to a spoofing service where it is bridged to a call with a new CPN, and returned via a VoIP call termination provider for connection back to a TDM-based called party on the PSTN.[28]

D. Caller Name Database Seeding

13. Many Caller ID services are able to display a name associated with the CPN, in addition to displaying the CPN itself.[29] Unlike the CPN, the name associated with the CPN is not transmitted by the originating carrier or provider. Instead, the terminating provider offering the Caller ID service uses the CPN to retrieve the name associated with the CPN from a Caller Name (CNAM) database.[30] CNAM databases link CPNs to the individuals and entities to whom the numbers have been assigned. Some terminating providers maintain their own CNAM database and others purchase CNAM database services from third-party providers that aggregate the listing information from a variety of sources. Typically this aggregation is done with real-time information feeds and may involve a chain of feeds through several layers of providers and

[26] *See, e.g.*, TelTech Comments at 21 n.11, WC Docket No. 11-39 (filed Apr. 18, 2011) ("[TelTech's] 'do not spoof' list, for example, contains over 4500 numbers, the majority being numbers provided by law enforcement agencies and most of the remainder coming from financial institutions.").

[27] *See* JSM Tele-Page Comments at 1, WC Docket No. 11-39 (filed Mar. 23, 2011).

[28] *See, e.g.*, Itellas Comments at 2, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239385.

[29] There can be multiple names associated with a given CPN in directory listings; for example, a wife and husband might be listed separately in the directory with the same telephone number. The name displayed is usually the "main" name listed for the telephone number.

[30] This is also referred to as "Calling" Name.

resellers.[31]

14. Although many CNAM database service providers deal with trusted sources and take pride in the accuracy of their information, standards vary and it is possible for bad actors to intentionally link phone numbers they control to misleading names in systems feeding some CNAM database services.[32] When that number is later used as the CPN on calls, the misleading caller name listing will be displayed if the corrupted CNAM database is queried. For example, as part of an identity theft scheme aimed at collecting consumers' bank account numbers, a fraud artist might arrange to associate the name, or a variation of a name, of a well-known bank with the phone number controlled by the fraud artist. Thus, the CPN that is displayed on the consumer's Caller ID device may be accurate, but because the name is intentionally misleading, the call recipient may be fooled into thinking that the call is from his or her bank, and provide account information and other sensitive personally identifiable information when asked.

E. Emergency Calling

15. An important type of caller identification service involves emergency calls to 9-1-1 services. As a general matter, calls that are placed to emergency services by dialing 9-1-1 are not highly vulnerable to spoofing. Emergency 9-1-1 calls do not rely on the CPN information used by Caller ID services described above either for routing or for retrieving the caller's location information. Instead, emergency 9-1-1 calling relies on a second number in the SS7 call setup information, generally referred to as the Automatic Number Identification (ANI).[33] Although the CPN and the ANI will typically be the same for residential, 9-1-1 calls are routed much differently from ordinary calls.[34] Although interconnected VoIP technology allows the ANI to be manipulated as easily as the CPN, it is in general difficult to get a call from the Internet with a spoofed ANI properly routed to a Public Safety Answering Point (PSAP) over the current Wireline E911 Network.[35]

16. A malicious actor can, however, spoof a call directly to other phone lines operated by

[31] TARGUSinfo, Remarks in an informational presentation to Federal Communications Commission staff (June 2009).

[32] *See, e.g.*, INCODE TELECOM GROUP, EVALUATING THE RELATIVE PERFORMANCE OF CALLER IDENTIFICATION SOLUTIONS (2008), *available at* http://www.verisign.com/static/CNAM_Accuracy_Report.pdf.

[33] The terms ANI and "Charge Number" are often used interchangeably to refer to the same piece of information, since the ANI is typically transmitted in the Charge Number parameter of the SS7 call setup message.

[34] When a 9-1-1 call is placed from a wireline phone, the LEC switch recognizes the dial string and routes the call setup information including the calling party number to an associated Selective Router. The Selective Router completes the call over 9-1-1 dedicated circuits to the appropriate PSAP based on the mapping of an ANI value to a particular PSAP as pre-set in the selective routing tables. These facilities constitute the Wireline E911 Network. As the E9-1-1 call taker at the PSAP answers the call, the ANI is sent in a query to the off-site ALI database. Emergency calls placed from mobile phones and many interconnected VoIP service phones require more complex processing involving a pseudo-ANI (pANI), although ultimately such calls rely on the same local routing information pre-set in the Selective Routers.

[35] *See* National Emergency Number Association (NENA) Comments at 3, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239909 ("NENA considers the probability that individual [sic] could successfully spoof ANI or pANI on a reproducible basis to be negligible.").

emergency service providers, such as a police department or fire department administration number. This case of emergency services being vulnerable to caller ID spoofing is particularly important in the small remaining areas of the United States where subscribers cannot reach emergency services by dialing 9-1-1 because the local telephone switching equipment does not recognize and handle the 9-1-1 dial sequence. In those few localities, the PSAPs may rely on the PSTN and consumer-grade Caller ID service described above, and thus may be subjected to the same caller ID spoofing associated with that service.[36]

III. TRUTH IN CALLER ID ACT

A. Implementing the Truth in Caller ID Act

17. As noted above, on December 22, 2010, President Barack Obama signed into law the Truth in Caller ID Act, which prohibits the intentionally harmful or fraudulent spoofing of caller identification information and gives the Commission the authority to seek substantial penalties from those who violate the Truth in Caller ID Act. The Truth in Caller ID Act requires the Commission to issue implementing regulations within six months of the law's enactment[37] and, as also noted previously, directs the Commission to submit this Report to Congress by the same date.

18. On June 22, 2011, the Commission issued rules implementing the Truth in Caller ID Act. These rules reflect Congress's directive to prohibit caller ID spoofing done with the intent to defraud, cause harm, or wrongfully obtain anything of value[38] by adding a section to the Commission's rules governing CPN services, and by enhancing the Commission's forfeiture rules.[39] The additions to the Commission's CPN rules are modeled on the Truth in Caller ID Act's prohibition against engaging in caller ID spoofing with fraudulent or harmful intent. The amendments to the Commission's forfeiture rules implement the forfeiture penalties and forfeiture process provided for in the Truth in Caller ID Act.

19. The Truth in Caller ID Act's prohibition is directed at spoofing "in connection with any telecommunications service or IP-enabled voice service."[40] Therefore, the Commission's rules define "caller identification service" and "caller identification information" in a manner that applies to calls using both types of service. Under the Commission's rules, the person or entity prohibited from knowingly causing transmission or display of inaccurate or misleading caller identification is the same person or entity that must be acting with intent to defraud, cause harm, or wrongfully obtain anything of value.

---

[36] *See* NENA Comments at 4, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239909. PSAP call takers who may be reached by dialing the conventional phone number of a PSAP administrative line, in addition to dialing 9-1-1, may also be vulnerable to the spoofing that is possible with consumer-grade Caller ID service.

[37] *See* 47 U.S.C. § 227(e)(3)(A).

[38] *Id.* § 227(e)(1) ("In General.—It 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 pursuant to paragraph (3)(B).").

[39] *See Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, FCC 11-100, paras. 13, 44 (June 22, 2011) (*Caller ID Act Order*).

[40] *See* 47 U.S.C. § 227(e)(1).

20. The rules address displaying inaccurate caller identification information, in addition to transmitting it, to make clear that even if no substitute CPN is transmitted between providers, it is a violation for a person or entity to knowingly cause a device that displays caller identification information to display inaccurate or misleading information with the intent to defraud, cause harm, or wrongfully obtain anything of value. This would include, for example, seeding a Caller Name database with a misleading listing name for the CPN used.

21. Although the Truth in Caller ID Act specifies that "IP-Enabled Voice Service" has the "meaning given that term by section 9.3 of the Commission's regulations (47 C.F.R. 9.3),"[41] the precise term used in 47 C.F.R. § 9.3 is "interconnected VoIP service." Hence, the Commission's rules implementing the Truth in Caller ID Act use the term "interconnected VoIP service" and specify that it has the same meaning given that term in 47 C.F.R. § 9.3. Although "telecommunications service" is defined by the Communications Act to mean the offering of telecommunications to the public for a fee,[42] there is no such commercial requirement for interconnected VoIP service. Therefore, an entity that self-provisions a VoIP service that interconnects with the PSTN in a manner that meets the criteria of section 9.3 is covered by the Truth in Caller ID Act.

22. The term "Caller Identification Service" in the Truth in Caller ID Act explicitly includes "automatic number identification services." The Commission rules define "caller identification service" to mean "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." The Commission clarified that by including billing number information in the definition of "information regarding the origination," it effectively includes within the definition of "caller identification service" any service or device designed to provide the user with any form of the calling party's billing number, including charge number, ANI, or pseudo-ANI.[43]

23. In the Commission's rulemaking proceeding, the Commission noted that some third-party spoofing service providers also offer separate services with the ability to unmask a CPN that the caller has affirmatively indicated should not be displayed. This unmasking is accomplished by reversing the privacy indicator initially set in accordance with the caller's privacy preference, and could be considered the "provision of inaccurate caller identification information" addressed by this Report. The Commission did not, however, receive public comment sufficient to enact rules concerning the intentional unmasking of caller identification information.[44]

B. Issues Raised by Commenters

24. As a result of the Commission's implementation of the Truth in Caller ID Act, the Commission's rules now address many of the vulnerabilities to caller ID spoofing used to defraud, cause harm, or wrongfully obtain anything of value as described in the Background section for current telecommunications voice services and interconnected VoIP voice services. However, stakeholders have identified several ways in which the Truth in Caller ID Act could be strengthened to improve protections against malicious caller ID spoofing. We discuss these in the sections that follow.

---

[41] 47 U.S.C. § 227(e)(8)(C).

[42] *See* 47 U.S.C. § 153(46).

[43] *See Caller ID Act Order*, FCC 11-, para. 31.

[44] *See* TelTech Comments at 19, WC Docket No. 11-39 (filed Apr. 18, 2011).

1. Malicious Spoofing Done from Outside the United States

25. The prohibition in the Truth in Caller ID Act against harmful or fraudulent caller ID spoofing applies to "any person *within the United States*" (emphasis added).[45] However, as at least one stakeholder in the FCC's proceeding has noted, spoofing also originates from people and entities operating outside the United States who may not be deterred or prevented from spoofing by the Commission's rules.[46] Indeed, caller ID spoofing directed at the United States by people and entities operating outside the country can cause great harm.[47]

2. Voice Services That Are Not "Telecommunications Services" or "Interconnected VoIP Services"

26. The Commission's rules implementing the Truth in Caller ID Act apply to spoofing done in connection with switched voice communications that qualify as "telecommunications service" or "interconnected VoIP service." However, a significant and growing amount of voice communications traffic today does not fall into either category. An important category is Internet-only non-interconnected VoIP service that enables users to engage in two-way voice conversations over the publicly-accessible Internet without interconnecting to the PSTN. In at least one instance, the Commission has declared such a service to be an information service and thus not subject to the Commission's rules governing CPN services.[48] Several commenters recommended ways in which the Commission should broaden the scope of its rules to include non-interconnected VoIP services.[49]

27. We note that the record does not demonstrate that caller ID spoofing concerns with consumer-grade, Internet-only non-interconnected VoIP services have risen to the same level as with interconnected VoIP services. The user of an Internet-only non-interconnected VoIP service typically establishes a contact list of the parties whom she will be calling and from whom she will

[45] 47 U.S.C. § 227(e)(1).

[46] *See* JSM Tele-Page Comments at 2, WC Docket No. 11-39 (filed Mar. 23, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021135004

[47] For example, the Federal Trade Commission in 2005 sued the operators of a bogus business opportunity scheme that was operating outside the United States, but using VoIP services to make it appear as if the company was based in the United States. *See* News Release, Federal Trade Commission, FTC Halts Bogus Business Opportunity Scam (Nov. 16, 2005), *available at* http://www.ftc.gov/opa/2005/11/usabeverage.shtm.

[48] *Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, 19 FCC Rcd 3307, 3311–14, paras. 11–17 (2003) (citing 47 U.S.C. §153(20)).

[49] *See* Letter from Lanny A. Breuer, Assistant Attorney General, U.S. Department of Justice, to Marlene H. Dortch, Secretary, FCC, at 4-5, WC Docket No. 11-39 (Jan. 26, 2011) (DOJ Jan. 26, 2011 Letter); NECA *et al*. Comments at 4–5, WC Docket No. 11-39 (filed Apr. 18, 2011) (agreeing with DOJ that the Commission should use a broader definition of IP-enabled voice services to ensure that caller ID requirements will apply to voice services, regardless of the network configuration used to connect customers and transport calls); Texas 911 Agencies Comments at 2–3, WC Docket No. 11-39 (filed Apr. 18, 2011) (agreeing with DOJ's suggestion for a broader definition of IP-enabled services to make clear that it covers VoIP services that arguably are not covered by the current definition of interconnected VoIP services); *see also* Alliance for Telecommunications Industry Solutions (ATIS) Comments at 4, WC Docket No. 11-39 (filed Apr. 18, 2011); AT&T Comments at 4–5, WC Docket No. 11-39 (filed Apr. 18, 2011); NENA Comments at 2, WC Docket No. 11-39 (filed Apr. 18, 2011).

accept calls.[50] An affirmative acceptance of a text-based request message by that party confirms permission to do so.[51] In this manner the universe of potential callers is greatly reduced, often to just friends and family. Optional real-time video capability likely further reduces the effectiveness of caller identification spoofing on Internet-based non-interconnected VoIP in instances where the personal account of an accepted contact might have been compromised.

28. There is a closely related category of VoIP service, however, that does facilitate caller ID manipulation on calls to subscribers of telecommunications services and IP-enabled services. This category includes one-way interconnected VoIP services, which are Internet based services that support the ability to place calls to end users of telecommunications services and interconnected VoIP services, but not to receive calls from those end users.[52] This class of service does not qualify as an interconnected VoIP service, as currently defined in the Commission's rules, because it does not permit "users generally to receive calls that originate on the public switched telephone network *and* to terminate calls to the public switched telephone network."[53] Because the device used by a subscriber to this class of service to originate calls is typically not assigned a telephone number, if a substitute CPN is provided by the subscriber it must necessarily be that of some other device or a non-working number.

29. Most recently, non-interconnected VoIP services have become available that allow direct, Internet-based global communications among enterprise customers that have their own VoIP-based corporate networks.[54] Typically such services assume the intervening network is untrustworthy and rely on sophisticated end-to-end authentication techniques to ensure the identity of the parties involved. We are not aware of caller ID spoofing concerns with these business-grade, non-interconnected VoIP services.

3. Third-Party Spoofing Services

30. Callers can easily engage in Caller ID spoofing by making use of one of the numerous third-party providers of caller ID spoofing services.[55] Third-party spoofing services can facilitate lawful instances of caller ID manipulation as well as unlawful caller ID manipulation. The Truth

[50] *See, e.g.*, Skype, *Calling someone who's on Skype* (2011), http://www.skype.com/intl/enus/support/user-guides/calling-someone-whos-on-skype/.

[51] *See, e.g.*, Skype, *How do I add contacts?* (2011), https://support.skype.com/en-us/faq/FA3281/How-do-I-add-contacts.

[52] Skype Call Phones service (previously known as SkypeOut) is one such service. *See* Skype, *How do I change my caller-identification settings?* (2011), https://support.skype.com/en-us/faq/FA2561/How-do-I-change-my-caller-identification-settings. By one estimate, Skype Call Phones service and Skype Online Number service (previously known as SkypeIn) accounted for almost 13 billion minutes of calls worldwide in 2010. *See* Press Release, TeleGeography, Microsoft's Acquisition of Skype (May 10, 2011), *available at* http://www.telegeography.com/press/press-releases/2011/05/10/microsofts-acquisition-of-skype/index.html. By way of comparison, the number of cell phone minutes of calls in the U.S. in 2010 is estimated at 2,241 billion. *See* CTIA, *Minutes and Messages as a Measure of Wireless Usage*, *in CTIA Semi-Annual Wireless Industry Survey*, fig. 7, CTIA (2011), *available at* http://files.ctia.org/pdf/CTIA_Survey_Year_End_2010_Graphics.pdf. Some VoIP services self-provisioned by the end user also may also fall into this category of VoIP services that enable calls to, but not from, the PSTN.

[53] 47 C.F.R. § 9.3 (emphasis added).

[54] *See, e.g.*, Verizon, *Verizon VoIP IP Enterprise Routing (VIPER)* (2010), http://www.verizonbusiness.com/resources/factsheets/fs_voip-ip-enterprise-routing_en_xg.pdf.

in Caller ID Act does not impose specific requirements on third-party spoofing services and, therefore, the Commission did not impose additional obligations on third-party spoofing services or VoIP call termination services at this time.[56] Some commenters recommended that third-party services should be held liable for knowingly facilitating malicious conduct,[57] and others recommended that the Commission impose obligations on third-party spoofing service including, for example, giving prominent notice concerning the Truth in Caller ID Act provisions,[58] verifying the right to use a substitute CPN,[59] and keeping records on customers and their service use.[60] The Commission clearly stated in the *Caller ID Act Order* that the decision not to impose additional obligations on third party caller ID spoofers in no way immunizes a third-party service provider from its obligation to comply with the Act.[61]

31. The Department of Justice ("DOJ") filed comments with the Commission describing spoofing services as a "hotbed of illegal activity that permit criminals to more effectively harm, harass, and defraud the public."[62] In an effort to reduce the use of third-party spoofing services for criminal activities and make it easier for law enforcement to track criminals that use caller ID spoofing services, DOJ asked the Commission to consider requiring spoofing providers to place a verification call to establish that callers have authority over the telephone numbers they seek to use. If callers cannot verify their right to use a particular phone number or elect not to participate in verification, DOJ's proposal would permit them to choose from a list of telephone numbers controlled by the spoofing provider, if the provider maintains such a number pool. Alternatively, DOJ suggested that the Commission develop a technological solution that would enable call recipients to determine that a call has been spoofed and would enable law enforcement to trace spoofed calls back to the spoofing provider.[63]

32. The Commission shares DOJ's concerns about the abuse of spoofing services by criminals and the law enforcement challenge of locating and prosecuting criminals who abuse

---

[55] *See supra* paras. 9–12 (noting the ease with which callers can engage the services of third-party spoofing providers).

[56] *See supra* note 22 for a description of VoIP termination service.

[57] *See, e.g.*, Voice on the Net Coalition Comments at 4–5, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238964.

[58] *See, e.g.*, National Network to End Domestic Violence Comments at 8–17, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239745.

[59] *See, e.g.*, Department of Justice Comments at 4, 7, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238849; Minnesota Attorney General Comments at 3, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238456.

[60] *See, e.g.*, Itellas Comments at 3, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239385

[61] *See Caller ID Act Order*, FCC 11-100, para. 42.

[62] Department of Justice Reply at 3, WC Docket No. 11-39 (filed May 3, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021345322.

[63] *See* Department of Justice Comments at 4, 7, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238849; Minnesota Attorney General Comments at 3, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238456 (supporting DOJ's proposal).

caller ID spoofing due to the anonymity provided by the caller ID spoofing services. In adopting rules to implement the Truth in Caller ID Act, the Commission recognized that requiring caller ID spoofing services to verify that users have the authority to use a substitute number would likely reduce the use of caller ID spoofing to further criminal schemes and could simplify law enforcement efforts to determine who is behind a caller ID spoofing scheme. At the same time, the Commission concluded that in crafting the Truth in Caller ID Act, Congress intended to balance the drawbacks of malicious caller ID spoofing against the benefits provided by legitimate caller ID spoofing. The Act prohibits spoofing providers, like all other persons and entities in the United States, from knowingly spoofing caller ID with malicious intent. But the Act does not impose additional obligations on providers of caller ID spoofing services. Based on its understanding of Congress's intent, the Commission did not impose additional obligations on third-party spoofing providers.[64]

IV. SUCCESSOR AND REPLACEMENT TECHNOLOGIES

A. Continued Migration to IP-enabled Voice and Voice with Video Technology

33. As suggested by Congress' attention to both telecommunications services and IP-enabled voice services with caller identification features, the two categories are closely coupled in terms of the voice service presented to the end user. IP-enabled voice technology is very much a successor to the TDM-based voice telecommunications technology, and worthy of continued attention in this context. It is estimated that over a quarter of the traditionally TDM-based voice telecommunication network has already been transitioned to IP-based technology, including more than half of the traffic exchanged among carriers in the core of the network (*i.e.*, inter-exchange traffic).[65] It is further estimated that by 2014 this number will increase from one quarter to as much as 60 percent as the technology transformation from TDM-based voice to IP continues to extend from the network core out to more and more end users.[66]

34. This trend suggests that as increasing numbers of current users of telecommunications services switch to VoIP-based services, they will have additional flexibility to manage their CPNs. We also expect non-interconnected VoIP services to continue to grow, especially for international calling. The largest non-interconnected VoIP provider, Skype, estimates that its non-interconnected VoIP voice minutes worldwide increased by 68 percent from 2009 to 2010 to 190 billion minutes.[67] By one estimate, about half of that 2010 traffic, 96 billion minutes, was international calling.[68] It is further estimated that Skype's international traffic volume grew by 39 billion minutes in 2010, more than twice the volume gain achieved by all telephone companies in the world combined.[69]

---

[64] *See Caller ID Act Order*, FCC 11- 100, para. 40.

[65] Fred Kemmerer, CTO, GENBAND, Remarks at an Informational Presentation to Federal Communications Commission Staff (Apr. 26, 2011), sourced from Heavy Reading IP Network Transformation Market Tracker.

[66] *Id.*

[67] This includes voice-only and voice-with-video calling.

[68] *See* Press Release, TeleGeography, Microsoft's Acquisition of Skype (Mar. 10, 2010), *available at* http://www.telegeography.com/press/press-releases/2011/05/10/microsofts-acquisition-of-skype/index.html.

[69] *Id.*

B. Text Messaging

35. Text messaging based on Short Message Service (SMS) technology is as vulnerable to caller ID spoofing as voice telecommunications service and IP-enabled voice service.[70] This is particularly relevant as the average monthly use of text messaging per subscriber has been increasing,[71] while mobile voice usage has been declining.[72] Some of the third-party services that provide caller ID spoofing of voice calls also provide text messaging spoofing services.[73] Text-message spoofing services are provided on web pages on which the sender enters the mobile phone number of the party to whom the text is to be sent, and a substitute mobile phone number from which it will appear that the text message was sent. Many mobile service providers also offer similar websites at which anyone can send text messages to the provider's subscribers. The "source" information is entered manually by the sender, with no verification of the sender's authority to use the number.

36. Additionally, many mobile service providers offer email gateways from the Internet so that email sent to a phone number at the provider's email domain address is directly delivered to that phone.[74] The source address of email is easily spoofed by using readily available and free text messaging websites, which provides another way to mislead the recipient of a text message.

C. Video Calling Using Telephone Numbers

37. Text communication, including text messaging and Internet-based chat, has long been an essential form of communications for the deaf and hard of hearing. In recent years, text-based communication among the deaf has been succeeded by Internet-based video communications that allow deaf and hard-of-hearing persons to communicate using sign language. In addition to providing interpreter-based relay calling between deaf and hearing persons, Internet-based Video Relay Service (VRS) providers and the Commission's Internet-based Telecommunications Relay Service (TRS) Numbering Directory support direct video calling between deaf users over the Internet using 10-digit phone numbers.[75] Commission rules specifically governing TRS facilities

[70] We note that the issue of whether text messaging is a telecommunications or information service is currently pending before the Commission. *See* Petition of Public Knowledge *et al.* for Declaratory Ruling Stating Text Messaging and Short Codes are Title II Services Subject to Section 202 Nondiscrimination Rules (filed Dec. 11, 2007).

[71] Between 2009 and 2010, the number of text messages sent in the U.S. increased by almost one-third, from 1,563 billion to 2,052 billion. *See* Press Release, CTIA-The Wireless Association, CTIA-The Wireless Association Announces Semi-Annual Survey Results (Mar. 22, 2011), *available at* http://ctia.org/media/press/body.cfm/prid/2062.

[72] Between 2009 and 2010, minutes of mobile voice use by the same user base dropped by about 1.5% from 2,275 billion minutes to 2,241 billion minutes. *Id*.

[73] *See, e.g.*, FAQ, SPRANKED (2009), http://www.spranked.com/faq.php ("Spranked.com allows you to send anonymous or spoofed SMS with a customised Sender ID"); *Spoof SMS!*, SPOOFCARD, http://www.spoofcard.com/sms ("Send a Spoof SMS FREE!").

[74] Pursuant to the provisions of the CAN-SPAM Act, the Commission has implemented certain restrictions on unwanted mobile service commercial messages sent directly to a mobile device using a provider domain name that has been posted on the FCC's wireless domain name list. *See* 47 C.F.R. § 64.3100.

[75] By "direct" we mean that these video calls are set up by a VRS provider using the 10-digit phone number, but do not transit the relay service itself. Direct video interoperability is available to users of a variety of different service providers using a variety of different videophone devices and applications.

subject those using SS7 technology to the Commission's CPN rules, and require the transfer of calling party identifying information such as the 10-digit number assigned to a deaf or hard-of-hearing VRS user's Internet-based video terminal.[76] Accurate CPN is important for logging missed calls and for call-back purposes, but because the two-way communication using sign language is by nature face-to-face, deceptive caller ID practices do not appear to be a major consumer issue in this form of exclusively Internet-based video communications.

D. Social Media

38. Social networking technology can be regarded as an important successor to telecommunications and IP-enabled voice technologies, especially for communications among social acquaintances who have previously relied on voice calling to keep in touch. It is estimated that as of December 2010 almost 70 percent of mobile service subscribers in the U.S. were using text messaging, and this number was growing at an annual rate of about 8 percent. By comparison, the number of mobile subscribers using social networking as of December 2010 is estimated to have been about 25 percent, and was growing at an annual rate of about 56 percent.[77] Similarly, the number of minutes spent on Facebook was estimated to reach about 42.1 billion minutes for the month of August 2010,[78] and can be compared with approximately 187 billion minutes of mobile voice communications for the same month.[79]

39. As with the user of an Internet-only non-interconnected VoIP service, the social network user typically establishes a contact list of the parties with whom she will be communicating, including an affirmative acceptance confirming permission to do so.[80] In this manner the universe of potential parties in contact with any single user can, in theory, be restricted to personal acquaintances. In practice, however, many users are not so selective and, because spoofed user accounts are not uncommon, identification deception is not uncommon either.[81]

40. Major social network providers offer users means by which to readily report identification spoofing to the social network service provider.[82] Telecommunications services in particular lack corresponding easily-accessed tools and, unlike social network providers that can

---

[76] *See* 47 C.F.R. § 64.604(b)(5)–(6)

[77] Mark Donovan, Senior Vice President of Mobile, comScore, The 2010 Mobile Year in Review – U.S. webinar (Mar. 11, 2011), *available at* http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Mobile_Year_in_Review_-_U.S.

[78] *See, e.g.*, Mark Walsh, comScore: *Facebook Takes Lead in Time Spent*, MEDIAPOST NEWS (Sept. 9, 2010), http://www.mediapost.com/publications/ ?fa=Articles.showArticle&art_aid=135476.

[79] The 187 billion minutes of use figure is obtained by dividing the 2,241 billion minutes for 2010 by 12. *See* Press Release, CTIA-The Wireless Association, CTIA-The Wireless Association Announces Semi-Annual Survey Results (Mar. 22, 2011), *available at* http://ctia.org/media/press/body.cfm/prid/2062. *See supra* note 72 (noting that mobile voice usage has declined, dropping by 1.5 percent from 2,275 billion to 2,241 billion between 2009 and 2010).

[80] *See, e.g.*, Facebook, *Friends: Adding friends and friends requests* (2011), http://www.facebook.com/help/new/?page=767.

[81] *See, e.g.*, Miguel Helft, *Facebook Wrestles with Free Speech and Civility,* N.Y. TIMES, Dec. 12, 2010, *available at* http://www.nytimes.com/2010/12/13/technology/13facebook.html.

[82] *See, e.g.*, Facebook, *Reporting a violation* (2011), http://www.facebook.com/help/?page=798.

unilaterally block reported offenders they believe to be in violation of their Acceptable Use Policies, telecommunications providers' ability to take similar action is more limited because of their common carrier obligations.

E. Next Generation 9-1-1

41. Today's emergency 9-1-1 voice calls are largely protected from spoofing harm by the technological artifacts of the Wireline E911 Network.[83] However, these protections will gradually diminish as the TDM-based technology of the Wireline E911 Network is replaced by IP-based network technology in the Next Generation 9-1-1 network (NG9-1-1). This migration should greatly increase the varieties and capabilities of communication with PSAPs, but the IP-based technology of the publicly accessible Internet on which NG9-1-1 is based brings with it many of the same vulnerabilities to caller identification spoofing associated with today's consumer-grade interconnected VoIP services.[84]

42. Given the popularity and ubiquity of SMS text messaging, enabling text message access to emergency services may be one of the first steps in moving beyond a voice-only emergency calling framework. SMS, however, has many limitations that will need to be addressed if it is to become a reliable means for emergency communications.[85] Not the least among these is the vulnerability of SMS text messaging technology to caller identification spoofing as described above.[86]

F. Caller Identification Technologies

43. The ability to easily manipulate caller identification information is largely a product of the transition of voice telephony from a closed system based on TDM and SS7 technology to an open system based on IP and, typically, SIP technology; by one estimate as much as 60 percent of PSTN calling will be based on IP technology by 2014.[87] Industry-consensus solutions for

---

[83] *See supra* paras. 15–16 (noting that it is "in general very difficult to get a call from the Internet with a spoofed ANI properly routed to a Public Safety Answering Point (PSAP) over the current Wireline E911 Network"); *see also* NENA Comments at 3, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239909.

[84] "Next Generation 9-1-1 ('NG9-1-1') will enable the public to seek emergency services through a variety of communications methods including IP-based voice, video, and text. These novel services will bring with them new challenges as we move beyond the calling party identification schemes inherited from the architecture of legacy wireline networks." NENA Comments at 1, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021239909.

[85] The Commission launched an extensive inquiry into the "Framework for Next Generation 911 Deployment," coincidentally on the day before the Truth in Caller ID Act was signed into law. *See Framework for Next Generation 911 Deployment*, PS Docket No. 10-255, Notice of Inquiry, 25 FCC Rcd 17869 (2010).

[86] *See supra* paras. 35–36 (recognizing that SMS text messaging technology "is as vulnerable to caller ID spoofing as voice telecommunications service and IP-enabled voice service," and that some "third-party services that provide caller ID spoofing of voice calls also provide text messaging spoofing services"). For an extensive discussion of the spoofing vulnerabilities of text message communication used for emergency calling, see generally *Texting to 9-1-1: Examining the Design and Limitations of SMS* (4G Americas, White Paper, Oct. 2010), *available at* http://www.4gamericas.org/documents/SMS%20to%20911%20White%20Paper%20Final%20October%202010.pdf.

[87] *See supra* para. 33 (estimating that by 2014, the amount of PSTN calling based on IP technology will approach 60 percent "as the technology transformation continues to extend from the network core out to

authenticating caller identification information in IP-based signaling have been defined but are not deployed.[88] They generally rely on proven cryptographic techniques similar to those used to authenticate web sites and email messages. Given the current mechanisms by which telephone numbers are allocated to and managed by an identifiable set of carriers, service providers, and resellers, the processes and cryptographic infrastructure on which these solutions rely should be within the realm of practicability at a service provider level (*i.e.*, rather than at the end-user level).[89]

44. Although this approach would not preclude all caller ID spoofing, it would enable a terminating provider to identify calling party information which had not been altered and to which the originating provider had been allocated the rights (or had been delegated the rights in turn), such as the calling party's number. In other words, the terminating provider would be able to identify calls for which the calling party information had not been spoofed with a very high degree of certainty. Such a determination would be useful for Caller ID service purposes and particularly valuable for law enforcement and public safety purposes.

45. Technology relying exclusively on the analysis of audio at the receiving end of a call is also a possible tool to help determine the provenance of a call.[90] For example, it appears possible through a combination of signal processing and machine learning to determine the traversal of calls through different networks (e.g., cellular, then VoIP, then PSTN), and to distinguish calls made from specific service providers.[91] Such technologies could provide particularly useful tools for tracing back calls laundered through various networks for which the caller identification had been manipulated.

V. RECOMMENDATIONS FOR CONSIDERATION BY CONGRESS

A. Consider Expanding the Truth in Caller ID Act

46. With the Truth in Caller ID Act, Congress took an important step toward re-securing the integrity of the telephone number as a reliable identifier of a call's origin. We recommend additional steps that can be taken toward this end as the TDM technology on which

---

more and more end users"); *see also* Fred Kemmerer, CTO, GENBAND, Remarks at an Informational Presentation to Federal Communications Commission Staff (Apr. 26, 2011), sourced from Heavy Reading IP Network Transformation Market Tracker.

[88] "The Internet Engineering Task Force (IETF) has also recognized the spoofing problem in interconnected VoIP services that Congress is seeking to prevent. As a result, the IETF adopted RFC 4474 ('Enhancements for Authenticated Identity Management in SIP'), which describes a solution to the problem of caller ID spoofing." InCharge Systems, Inc. Comments at 2, WC Docket No. 11-39 (filed Apr. 13, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021237895.

[89] *See* JSM Tele-Page Comments at 2, WC Docket No. 11-39 (filed Mar. 23, 2011) ("Another approach to this problem might be to limit the 'spoofing' of Caller ID to those number resources assigned to the originating carrier by the North American Numbering Plan Administration.").

[90] *See* Telineage Comments at 2, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/ document/view?id=7021238709 ("The research shows that regardless of the claimed source, the audio delivered to a call recipient exhibits measurable features of the source and the networks through which the call was delivered.").

[91] *See, e.g.*, Vijay A. Balasubramaniyan *et al.*, *PinDr0p: Using Single-Ended Audio Features To Determine Call Provenance* (Converging Infrastructure Sec. Lab., Georgia Tech. Info. Sec. Ctr., Georgia Inst. of Tech., Research Paper, Oct. 2010), *available at* http://www.cc.gatech.edu/~traynor/papers/traynor-ccs10.pdf.

telecommunications service is widely based is increasingly supplanted by VoIP technology, and as text messaging continues to supplement and replace voice communications.

- **Recommendation 1: Congress should consider broadening the scope of the Truth in Caller ID Act to include a prohibition on caller ID spoofing directed at people in the United States by persons outside the United States.**

47. Caller ID spoofing directed at persons within the United States by people and entities operating outside the country can cause great harm, but such people and entities are not covered by the Truth in Caller ID Act.[92] In the past, Congress has recognized the need to expand the Commission's consumer protection authority to address entities outside the U.S. that direct their actions to the U.S. For example, as part of the CAN SPAM Act of 2003, Congress amended section 227(b) of the Act, which deals with auto dialing, prerecorded calls, and junk faxes, to cover any persons within the United States, or any person outside the United States if the recipient is within the United States.[93] Previously that section only applied to any person within the United States.

- **Recommendation 2: Congress should consider providing guidance whether it intended additional IP-enabled voice services, such as VoIP services that enable callers only to make outgoing calls to users of telecommunications and interconnected VoIP services, to be brought within the scope of the Truth in Caller ID Act.**

48. As explained above, the Truth in Caller ID Act applies to interconnected VoIP services as defined in section 9.3 of the Commission's rules, "as those regulations may be amended by the Commission from time to time."[94] The Commission thus has a specific delegation of authority to amend its definition of interconnected VoIP services so that the scope of the Truth in Caller ID Act would include one-way interconnected VoIP services, even though such one-way interconnected VoIP services are not currently covered.[95] As explained above, such services can be used as readily as telecommunications services and (two-way) interconnected VoIP services to spoof Caller ID. Indeed, several commenters recommended that the scope of the Act should be interpreted to reach services not currently within the Commission's definition of interconnected VoIP services—a view the Commission did not adopt.[96] Because expansion of the reach of the Truth in Caller ID Act to one-way interconnected VoIP services via a revision to Rule 9.3 would be a significant change, as to which Congress has not provided any specific indication of its intent, Congress may want to consider providing guidance whether it intends for the Truth in Caller ID Act to apply to calls made with such additional IP-enabled voice services.

---

[92] *See supra* para. 25 (noting that while malicious caller ID spoofing performed by perpetrators acting outside the U.S. can cause significant harm to victims within the U.S., these bad actors are not covered by the Truth in Caller ID Act).

[93] "SEC. 12. Restrictions On Other Transmissions. Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting ', or any person outside the United States if the recipient is within the United States' after 'United States')." CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified as 15 U.S.C. § 7701, *et seq*.).

[94] *See supra* para. 21; 47 C.F.R. § 9.3; 47 U.S.C. § 227(e)(8)(C).

[95] As explained *supra* para. 28, one-way interconnected VoIP services are Internet based services that support the ability to place calls to end users of telecommunications services and interconnected VoIP services, but not to receive calls from those end users.

[96] *See supra* paras. 26–28.

- **Recommendation 3: Congress should consider giving the Commission appropriate authority to regulate third-party spoofing services.**

49. As explained above, third-party spoofing services make it easy for anyone to spoof Caller ID for legal or illegal purposes. Granting the Commission additional specific authority over third-party providers of spoofing services may aid the Commission in enforcing its rules and promulgating additional rules to implement the Truth in Caller ID Act.[97] As discussed above, DOJ recommended that the Commission require third-party spoofing providers to verify that a user has authority to use the telephone number the user is seeking to have substituted for the user's calling number. DOJ's proposal would make it far easier for law enforcement to identify those actors who use third party spoofing services for fraudulent or other harmful purposes and permit caller ID spoofing for some legitimate purposes. In light of the serious and weighty concerns identified by DOJ involving law enforcement's need to track criminals who use third party caller ID spoofing services, we recommend that Congress revisit the Truth in Caller ID Act's apparent acceptance in some instances of the practice of spoofing phone numbers that the caller lacks authority to use, including granting the Commission appropriate authority to adopt rules preventing third-party spoofing providers from allowing unauthorized use of substitute phone numbers.

- **Recommendation 4: Congress should consider modifying the Truth in Caller ID Act to explicitly state that text messaging is covered by the scope of the Truth in Caller ID Act.**

50. We have observed that the use of SMS-based text messaging service is growing faster than cellular voice service and is subject to many of the same caller identification manipulation vulnerabilities as voice calling.[98]

B. Monitor New and Emerging Communications Services

51. Once the Commission's rules are in force, Congress and the Commission will have the opportunity to determine whether the current rules are sufficient to deter malicious caller ID manipulation in conjunction with telecommunications services and interconnected VoIP services. Congress and the Commission should monitor industry efforts to deploy existing industry-consensus solutions for authenticating caller identity, including the caller party's number, in IP-based communications services, with a particular eye toward identifying those aspects for which regulation may be required to prevent misuse or abuse.[99]

[97] *See* Department of Justice Comments at 9, WC Docket No. 11-39 (filed Apr. 18, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021238849.

[98] *See supra* paras. 35–36, and 42.

[99] *See supra* paras. 43–44.