Journal of Law and Policy

Volume 19 | Issue 2 Article 7

2011

Phoney Business: Successful Caller ID Spoofing Regulation Requires More Than the Truth in Caller ID Act of 2009

Alicia Hatfield

PHONEY BUSINESS: SUCCESSFUL CALLER ID SPOOFING REGULATION REQUIRES MORE THAN THE TRUTH IN CALLER ID ACT OF 2009

*Alicia Hatfield**

I. INTRODUCTION

In 2008, Doug Bates had a terrifying experience when he was forced to defend his home against what he thought were prowlers.[1] After putting his two toddlers to sleep, he and his wife heard noises coming from their backyard.[2] He grabbed a knife and faced the dark to defend his family.[3] Once outside, he quickly found himself blinded by a spotlight and disoriented by a booming command to drop the knife from his hand.[4] As he was tackled to the ground, he wondered what could possibly have caused a SWAT team to surround his home.[5] The answer to that question was Randal Ellis.[6]

---

* J.D. Candidate, Brooklyn Law School, 2012; B.A., Philosophy, Brooklyn College, 2008. I would like to thank my family and friends for their love and encouragement, especially my husband. I would also like to thank the faculty of Brooklyn law school and the editors and staff of the *Journal of Law and Policy* for their efforts on this note, especially Lindsay Lieberman for our many meetings. A special thanks is due to Steven Helfont for his editing and advice. Finally, I would like to thank the practitioners who contributed to this note, Mark Del Bianco and Jerry Grant.

[1] Salvador Hernandez, *Lake Forest Family Thankful '911' Hacker Going to Prison*, ORANGE CNTY. REG., Mar. 27, 2008, http://www.ocregister.com/news/family-185237-bates-home.html.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *See id.*

[6] Hernandez, *supra* note 1.

Just moments before, Ellis placed a call to 911 with "spoofed" caller identification ("caller ID") information, making the call appear to have originated from within Mr. Bates' home, a practice known as "swatting."[7] After Ellis told the dispatcher that drugs led him to murder his sister, the SWAT team was deployed to Mr. Bates' quiet California home.[8] Fortunately, the SWAT team handled the situation with caution and no one was injured.[9] While swatting is one of the many illegitimate uses of caller ID spoofing technology that has garnered significant media attention in recent years,[10] there are many legitimate and socially desirable uses of the technology.[11] Nonetheless, Congress introduced multiple anti-caller ID spoofing bills beginning in 2006.[12]

The Truth In Caller ID Act of 2009 ("TICIDA"), which outlaws the use of caller ID spoofing with intent "to defraud, cause harm, or wrongfully obtain anything of value," was signed into law

---

[7] *SWAT Teams Deployed in 911 Telephone Fraud*, MSNBC (Feb. 1, 2009, 4:55 PM), http://www.msnbc.msn.com/id/28965633/.

[8] *See id.*

[9] Hernandez, *supra* note 1. Ellis was sentenced to three years in prison. *Id.*

[10] *See generally* 152 CONG. REC. H3386, H3388 (daily ed. June 6, 2006) (statement of Rep. Engel). Most citizens trust the information displayed on caller ID devices since most remain unaware that caller ID spoofing technology exists. *Id.*

[11] *See* Part II.B.1 (describing the many legitimate uses of caller ID spoofing); *see also* 155 CONG. REC. S170, S173–74 (daily ed. Jan. 7, 2009) (statement of Sen. Nelson) (highlighting various illegitimate and legitimate uses).

[12] *See* Truth in Caller ID Act of 2010, H.R. 1258, 111th Cong. (2010); Truth in Caller ID Act of 2009, S. 30, 111th Cong. (2009); Preventing Harassment Through Outbound Number Enforcement Act of 2009, H.R. 1110, 111th Cong. (2009); Truth in Caller ID Act of 2007, S. 704, 110th Cong. (2008); Preventing Harassment Through Outbound Number Enforcement Act of 2007, H.R. 740, 110th Cong. (2007); Truth in Caller ID Act of 2007, H.R. 251, 110th Cong. (2007); Truth in Caller ID Act of 2006, S. 2630, 109th Cong. (2006); Preventing Harassment Through Outbound Number Enforcement Act, H.R. 5304, 109th Cong. (2006); Truth in Caller ID Act of 2006, H.R. 5126, 109th Cong. (2006). Many states have also proposed or passed laws making the act of caller ID spoofing illegal. *See generally* Margaret Stolar & Chuck Gall, *Bills Introduced to Battle Caller ID Spoofing*, 13 CONSUMER FIN. SERVS. L. REP. 5 (2009).

on December 22, 2010.[13] However, successful caller ID spoofing regulation requires more than a statute outlawing illegitimate uses of the technology, most of which were already illegal under existing federal laws. It is imperative that the Department of Justice, the Federal Communications Commission ("FCC"), and Congress accomplish effective regulation of the industry to curb the nefarious aspects of spoofing and preserve legitimate uses. This Note argues that the TICIDA cannot successfully regulate the caller ID spoofing industry because the criminal penalties under the TICIDA are too minimal to deter most illegitimate users; the TICIDA does not expressly criminalize text message spoofing; and the TICIDA does not create comprehensive regulation of the caller ID spoofing industry. In order to maintain the availability of this technology for legitimate users,[14] the Department of Justice should creatively and aggressively prosecute illegitimate users under alternative federal laws when doing so would result in greater deterrence. In addition, the FCC should request that Congress modify the TICIDA to define the term "call" as both voice and text calls expressly so that text message spoofing does not become a successor technology. Lastly, the FCC should promulgate regulations that facilitate the tracing of spoofed calls and create a Do-Not-Spoof list. Part II explains caller ID spoofing and highlights its most common legitimate and illegitimate uses. Part III analyzes state and federal attempts at anti-caller ID spoofing legislation. Part IV suggests steps the Department of Justice, the FCC, and Congress should take in order to maximize deterrence of illegitimate uses and create successful regulation of the caller ID spoofing industry.

II. BACKGROUND

A. What is Caller ID Spoofing?

To understand how caller ID spoofing is accomplished, it is

[13] Truth in Caller ID Act of 2009, S. 30, 111th Cong. (2009).

[14] *See generally* 156 CONG. REC. H2522 (daily ed. Apr. 14, 2010) (statement of Rep. Boucher) (explaining that the TICIDA is intended to outlaw nefarious uses but permit legitimate uses).

helpful to first understand traditional caller ID service. When a phone call is placed over the public switched telephone network[15] or on a cell phone, information about the phone call is sent along with the call itself to the called party.[16] The calling party number ("CPN"), one type of data sent with the call, is a ten-digit number that identifies the phone number from which the call is being placed.[17] If the called party subscribes to a caller ID service, the receiving phone company searches its records for the name that corresponds with the incoming CPN,[18] and the caller ID device displays that information.[19] If the caller blocks her caller ID information by dialing *67 before the called party's number, the CPN will include a marker to communicate to the receiving phone company that the call is intended to be anonymous.[20] In this case, the receiving phone company will not display the caller's CPN information.[21]

Another piece of information sent along with a phone call is the automatic number identification ("ANI").[22] The ANI also contains the ten-digit caller number; however, it is not used for caller ID purposes.[23] This information is sent with the phone call regardless of whether the caller utilized *67 call blocking.[24] The ANI enables premium phone services, such as 800 and 900 numbers, to identify which telephone account to charge for

---

[15] The public switched telephone network ("PSTN"), or the plain old telephone service, is the structure that transmits landline phone calls. HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 667 (20th ed. 2004); *see also* David Roos, *How Telephone Country Codes Work*, HOWSTUFFWORKS, http://communication.howstuffworks.com/telephone-country-codes1.htm (last visited Feb. 4, 2011).

[16] 47 C.F.R. § 64.1601(a) (2006).

[17] NEWTON, *supra* note 15, at 148.

[18] Ward Mundy, *Asterisk Caller ID Perfected: Caller ID Superfecta 2.0*, NERD VITTLES (May 11, 2009), http://nerdvittles.com/?p=609.

[19] *How Does Caller ID Work?*, HOWSTUFFWORKS, http://www.howstuffworks.com/question409.htm (last visited Feb. 4, 2011).

[20] 47 C.F.R. § 64.1601(b) (2006).

[21] *Id.*

[22] NEWTON, *supra* note 15, at 63.

[23] *Id.* at 147.

[24] *Id.* at 63.

incoming phone calls.[25] When caller ID information is spoofed, both the ANI and the CPN are changed to a fake phone number.[26]

1. Traditional Caller ID Spoofing

Primitive forms of caller ID spoofing were possible if the spoofer had sufficient knowledge of the telephone system to manipulate the signals that communicate caller ID information to the caller ID device.[27] The creation of voice over IP ("VoIP") technology[28] and the availability of web-based commercial spoofing companies has made caller ID spoofing more accessible.[29] When spoofing is accomplished via a commercial spoofing company, the spoofer first pays for a block of minutes in advance to establish an account.[30] To place a spoofed call, the spoofer either calls the company's 800 number or visits its website.[31] Next, the spoofer enters the number he is calling, followed by the number he would like displayed as the fake caller

---

[25] *Id.*

[26] *See The Truth in Caller ID Act: Hearing on H.R. 251 Before the Subcomm. on Telecomm. & the Internet of the H. Comm. on Energy & Commerce*, 110th Cong. 25 (2007) [hereinafter *Knight Statement*] (statement of Allison Knight, Staff Counsel, Electronic Privacy Information Center).

[27] S. REP. NO. 110-234, at 2 (2007). Spoofers created false caller ID tones to trick the caller ID device via software or recording a caller ID signal they wished to emulate. AOH Staff & dethme0w, *Orange Boxing/Caller ID Hacking FAQ*, ART OF HACKING (Oct. 21, 2006), http://www.artofhacking.com/files/OB-FAQ.HTM.

[28] *Voice-Over-Internet Protocol*, FED. COMM. COMM'N, http://www.fcc.gov/voip/ (last updated Feb. 1, 2010). VoIP is an alternative to traditional phone service that utilizes the Internet to place phone calls. *Id.*

[29] S. REP. NO. 110-234, at 2; *see also* Judy L. Thomas, *'Spoofers' Sidestepping Caller ID Raise Alarm*, ORLANDO SENTINEL, Sept. 20, 2009, http://articles.orlandosentinel.com/2009-09-20/news/0909200100_1_caller-id-called-spoofing-phone-calls (noting that the number one spoofing company, SpoofCard, has over three million customers).

[30] *Frequently Asked Questions*, SPOOFCARD, http://www.spoofcard.com/faq (last visited Feb. 4, 2011).

[31] *See* SPOOFCARD, http://www.spoofcard.com/ (last visited Feb. 4, 2011) (enabling users to place spoofed phone calls from the main page of the website).

ID number.[32] Depending on the service used, the spoofer may also have the option to record the call or to alter the sound of his voice.[33] It is impossible to trace spoofed calls except by subpoenaing the spoofing company's records to determine the identity of the customer.[34]

Spoofing is also possible for individual users of VoIP services.[35] VoIP technology utilizes a text-based method for initiating and ending a phone call, known as Session Initiation Protocol ("SIP").[36] Spoofing is accomplished when the spoofer uses software, often a program known as Asterisk, to alter his SIP information.[37] Multiple websites provide step-by-step instructions for this process.[38] Most VoIP providers prevent their users from altering their SIP information,[39] but some providers do not secure their systems.[40]

2. Text Message Caller ID Spoofing

Text message spoofing takes place when a party changes the "from" information in a text message so that it appears that the text message was sent from a different telephone.[41] In this way, text

---

[32] *Frequently Asked Questions*, *supra* note 30.

[33] 155 CONG. REC. S170, S173 (2009) (daily ed. Jan. 7, 2009) (statement of Sen. Nelson).

[34] Thomas, *supra* note 29. Spoofcard reports that it is highly cooperative with law enforcement efforts to stem illegal uses of the technology. *Id.*

[35] VonageTPA, Comment to *Caller ID Spoofing*, VONAGE VOIP F. (Mar. 2, 2006, 12:35 AM), http://www.vonage-forum.com/ftopic11704.html.

[36] NEWTON, *supra* note 15, at 752.

[37] Mundy, *supra* note 18.

[38] VonageTPA, *supra* note 35; *see also Reports: Automated Caller ID/ANI Spoofing*, ROOTSECURE.NET (July 8, 2004), http://www.rootsecure.net/?p=reports/callerid_spoofing.

[39] *See* VonageTPA, *supra* note 35. Vonage is an example of a company that prevents users from altering SIP information. *Id.*

[40] Ward Mundy, *Asterisk Caller ID on Steroids: Here's How*, NERD VITTLES (Feb. 9, 2006), http://nerdvittles.com/index.php?p=115 (claiming VoIP providers TelaSIP and Teliax are among the few that still allow caller ID manipulation).

[41] E-mail from Jerry Grant, JR Computer Consulting, to author (Sept. 19,

message spoofing is similar to caller ID spoofing, except that it affects mobile phones exclusively. Text message spoofing is usually accomplished through a text message spoofing website, often owned by the same companies that own caller ID spoofing websites.[42] The only way to verify that the text message was spoofed is to look at the alleged sender's phone records for the absence of the outgoing message.[43]

B. Uses of Caller ID Spoofing

Caller ID spoofing has many uses.[44] Although some states' approach to caller ID spoofing classifies all caller ID spoofing as illegitimate, Congress has recognized legitimate uses. The floor debates on the TICIDA evince a Congressional intent to secure the availability of the technology for legitimate users.[45] This section discusses which uses Congress labeled as legitimate and illegitimate.

1. Legitimate Uses of Caller ID Spoofing

There are many legitimate users of caller ID spoofing, including business professionals who use the technology to prevent their personal numbers from becoming public and call centers that project incoming phone numbers on their outgoing lines.[46] Doctors

---

2010, 9:11 AM) (on file with author).

[42] *Id.*

[43] *Id.*

[44] *E.g.*, 153 CONG. REC. E1286 (daily ed. June 13, 2007) (statement of Rep. Green).

[45] *See, e.g.*, 152 CONG. REC. H3386, H3387 (daily ed. June 6, 2006) (statement of Rep. Markey) (stating the importance of protecting legitimate uses); 156 CONG. REC. H2522, H2523 (daily ed. Apr. 14, 2010) (statement of Rep. Boucher) (asserting that domestic violence survivors do not intend to deceive when using caller ID technology, so their use would not be criminalized under H.R. 1258).

[46] *See, e.g.*, 156 CONG. REC. H2522–24 (statement of Rep. Boucher); 152 CONG. REC. H3386, H3387 (statement of Rep. Markey). By spoofing, telemarketing companies are able to provide the recipients of their calls with a viable return number. *The Truth in Caller ID Act: Hearing on S. 704 Before the*

and other professionals, who must make occasional phone calls from home, use the service to project their office numbers, informing their clients that they are calling while keeping their private numbers undisclosed.[47] Teltech Systems, Inc. ("Teltech")[48] reports that the service is also useful for journalists who want to keep their personal numbers private.[49] Additional uses of caller ID spoofing include "seeking criminals who have jumped bail, tracking down child support payment deadbeats, . . . providing whistleblowers anonymity in making disclosures,"[50] and facilitating debt collection.[51] Even Congress members use the technology so that outgoing calls display the office's main number instead of the numbers of their personal lines.[52]

Arguably, the most socially valuable use of spoofing technology is to protect domestic violence shelters and victims, and this has long been a congressional priority when dealing with caller ID technology.[53] In 1995, the FCC passed regulations requiring that individual users have the capability to block their

---

S. Comm. on Commerce, Sci., & Transp., 110th Cong. 5 (2007) [hereinafter *Cerasale Statement*] (statement of Jerry Cerasale, Senior Vice-President, Direct Marketing Association). If a consumer attempted to return a telemarketing call to an outgoing line, the number would be busy. *Id.*

[47] *See, e.g.*, 153 CONG. REC. H6257, H6258 (daily ed. June 12, 2007) (statement of Rep. Markey); *Cerasale Statement*, *supra* note 46.

[48] Teltech is the parent company of SpoofCard, the largest caller ID spoofing company. Thomas, *supra* note 29.

[49] Plaintiff's Statement of Material Facts in Support of Motion for Summary Judgment at 3, Teltech Sys., Inc. v. McCollum, No. 08-61664-CIV-Martinez-Brown (S.D. Fla. 2009).

[50] Drew Douglas, *Marketers Challenge Constitutionality of Florida's Caller ID Spoofing Ban*, 9 COMPUTER TECH. L. REP. (BNA) 550 (Nov. 7, 2008). The TICIDA contains a law enforcement exception, ensuring that law enforcement may legally continue to use caller ID spoofing. Truth in Caller ID Act of 2009, S. 30, 111th Cong. § 2(e)(3)(ii) (2009).

[51] *The Truth in Caller ID Act: Hearing on S. 704 Before the S. Comm. on Commerce, Sci., & Transp.*, 110th Cong. 5 (2007) [hereinafter *Monteith Statement*] (statement of Kris Monteith, Chief of Enforcement Bureau, FCC).

[52] 153 CONG. REC. H6257, H6258 (daily ed. June 12, 2007) (statement of Rep. Markey).

[53] *See id.*

personal information when making calls by dialing *67.[54] Many states introduced regulations that required blocking options to be provided free of charge, partially out of concern for domestic violence victims.[55] Thus, government officials have consistently tried to minimize the likelihood that caller ID could deliver the location of a domestic violence victim or shelter to her abuser.[56] By using caller ID spoofing, victims are able maintain contact with loved ones safely.

2. Illegitimate Uses of Caller ID Spoofing

Caller ID spoofing also has many nefarious uses.[57] Proponents of caller ID spoofing legislation focused on particularly egregious examples of illegitimate uses during debates.[58] This section discusses the four nefarious uses of spoofing technology most

---

[54] 47 C.F.R. § 64.1601(b) (2006).

> Carriers must arrange their CPN-based services, and billing practices, in such a manner that when a caller requests that the CPN not be passed, a carrier may not reveal that caller's number or name, nor may the carrier use the number or name to allow the called party to contact the calling party.

Id.

[55] *Telephone Firms Give in on Caller-ID Blocking*, NEWSDAY, Oct. 9, 1990, at 41; *see also* Timothy C. Barmann, *Cox Communications Cancels Plans to Charge for Privacy Service*, PROVIDENCE J., Jan 9, 2001.

[56] *See, e.g.*, Bob Wyss, *Wires Crossed in Caller ID Blocks Phone Companies Promise Privacy, but Failures Abound*, PROVIDENCE J., March 5, 1995, at 1A; *Telephone Firms Give in on Caller-ID Blocking*, *supra* note 55. Opponents of caller ID forcefully argued that the service made customers vulnerable by releasing their private information without regard to whether the customer wanted to enroll in the service, and that this was particularly dangerous in the context of domestic violence shelters and victims. *Telephone Firms Give in on Caller-ID Blocking*, *supra* note 55.

[57] *The Truth in Caller ID Act of 2006: Hearing H.R. 5126 Before the Subcomm. On Telecomms. & the Internet of the H. Comm. on Energy & Commerce*, 109th Cong. 24 (2006) (statement of Lance James, Chief Technology Officer, Secure Science Corp.). It is estimated that in excess of seventy-five percent of spoofed calls are made for malicious purposes. *Id.* at 25.

[58] *See, e.g.*, 156 CONG. REC. H2522–24 (daily ed. Apr. 14, 2010) (statement of Rep. Boucher).

often cited by proponents during debates on the TICIDA: fraud,[59] swatting,[60] harassment,[61] and political harassment.[62]

i. Fraud

Caller ID spoofing is used to perpetrate fraud in two ways: to make victims believe a spoofer is a trusted entity or to make a trusted entity believe a spoofer is his victim.[63] In other words, caller ID spoofing can be used either to trick a victim into revealing confidential information, often called phishing, or to verify identity fraudulently when calling an institutional entity.[64] Phishers use their fraudulently gained information to transfer money from bank accounts, to sell credit card numbers to third parties, or to apply for credit cards or loans in their victim's name.[65] Microsoft research estimates that phishers stole over $61 million in 2007.[66]

Traditionally, phishers used spoofed websites or emails to trick users into entering confidential usernames and passwords.[67] Now, phishers can also use spoofed caller ID information.[68] In Sterling,

---

[59] *See id.*

[60] *See, e.g.*, 155 CONG. REC. S170, S173 (daily ed. Jan. 7, 2009) (statement of Sen. Nelson).

[61] *See, e.g.*, *Native American Methamphetamine Enforcement, The Animal Fighting Prohibition Enforcement Act of 2007, and the Preventing Harassment Through Outbound Number Enforcement (PHONE) Act of 2007: Hearing on H.R. 545, H.R.137, & H.R. 740 Before Subcomm. On Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 110th Cong. 27 (2007) [hereinafter *Sabin Statement*] (statement of Barry Sabin, Deputy Asst. Att'y Gen., Criminal Div., U.S. Dep't of Justice).

[62] *See, e.g.*, 156 CONG. REC. H2522, H2524 (daily ed. Apr. 14, 2010) (statement of Rep. Stearns).

[63] *See generally* 2 RICHARD RAYSMAN & PETER BROWN, COMPUTER LAW: DRAFTING AND NEGOTIATING FORMS § 15.05 (2010).

[64] *Id.*

[65] Jeremy Feigelson & Camille Calman, *Liability for the Costs of Phishing and Information Theft*, 13 no. 10 J. INTERNET L., Apr. 2010, at 16.

[66] *Id.* at 17.

[67] RAYSMAN & BROWN, *supra* note 63.

[68] S. REP. NO. 110-234, at 1–2 (2007).

Michigan, for example, residents received phone calls appearing to originate from the local courthouse.[69] Victims were told they had "missed jury duty" and they would be arrested if they did not immediately provide their Social Security number.[70]

Caller ID spoofing is also used to fraudulently verify identity to gain access to confidential accounts.[71] For example, Western Union has proceeded with cash transfers after credit card thieves spoofed the credit card holder's caller ID information, making the call appear to have been placed by the individual whose identity was stolen.[72]

Voicemail hacking is another example of fraudulently verifying identity.[73] Many voicemail companies provide users access to their mailbox via caller ID verification without requiring a password.[74] This security flaw was famously exposed in 2006, when SpoofCard[75] suspended over fifty accounts, including socialite Paris Hilton's, because of suspected voicemail hacking activity.[76] Notwithstanding the account suspensions, the Los Angeles District Attorney investigated voicemail hacking in 2008 after receiving complaints.[77] Ultimately, SpoofCard's parent company agreed to a permanent injunction, requiring that it may no longer advertise that it is "legal in all 50 states, if that is not the

---

[69] *Id.*

[70] *Id.*

[71] *See, e.g.*, 155 CONG. REC. S170, S173 (daily ed. Jan. 7, 2009) (statement of Sen. Nelson).

[72] S. REP. NO. 110-234, at 2.

[73] *See* Tom Gilroy, *Software Firm, Two Cell Phone Providers Settle DA's Allegations of Illegal 'Spoofing,'* 9 COMPUTER TECH. L. REP. (BNA) 616 (Dec. 19, 2008).

[74] *Id.*

[75] Spoofcard is the largest spoofing company, with over three million customers. Thomas, *supra* note 29.

[76] Robert McMillan, *Paris Hilton Accused of Voice-Mail Hacking*, INFOWORLD (Aug. 25, 2006), http://www.infoworld.com/d/security-central/paris-hilton-accused-voice-mail-hacking-457. Many gossip columns reported that Hilton used the technology to hack into actress Lindsay Lohan's voicemail, although Hilton's spokesman denied the allegations. *Id.*

[77] Gilroy, *supra* note 73.

case . . . ."[78] In addition, T-Mobile and AT&T were enjoined from advertising that pin-free voicemail access was a secure method of verification.[79] Despite these efforts, voicemail hacking still occurs.[80] In April 2010, the former publicity director for Dolce & Gabbana, Ali Wise, faced up to four years in prison but instead pleaded guilty to hacking into at least four people's voicemail accounts, listening to and deleting their messages.[81]

ii. Swatting

Swatting occurs when a spoofed call is placed to an emergency number.[82] The caller claims that an emergency is taking place at the location of the spoofed number.[83] This process is known as swatting because the goal is to cause the deployment of a SWAT team to the location from which the call appears to originate.[84] In 2009, for example, police caught a group of men who had prank called over sixty cities, claiming that hostage situations were in progress.[85] The scheme cost the cities over $250,000 in emergency response expenses, claimed over 250 victims, and injured two.[86]

Emergency service prank calls have serious implications. The calls can overload the emergency response system itself, and can prevent police officers from responding to legitimate calls.[87]

---

[78] *Id.*

[79] *Id.*

[80] Laura Italiano, *PR Princess Ali Wise Pleads Guilty to Felony Charge*, N.Y. POST, Apr. 29, 2010, http://www.nypost.com/p/news/local/manhattan/charge_princess_ali_wise_agrees_NQ0hSsbdOjUH4cA4n0mLkO.

[81] *Id.* Ms. Wise hacked into one victim's voicemail over 337 times. *Id.*

[82] Steve La, *Prank Calls to SWAT No Joke to L.A. County Sheriffs*, LA WEEKLY BLOGS (Aug. 30, 2010, 12:10 PM), http://blogs.laweekly.com/informer/2010/08/prank_calls_to_swat_is_no_joke.php.

[83] *Id*.

[84] *Guadalupe Santana Martinez Sentencing Press Release*, U.S. DEP'T OF JUSTICE (Mar. 12, 2008), http://www.justice.gov/usao/txn/PressRel08/martinez_guadalupe_swat_sen_pr.html.

[85] Thomas, *supra* note 29.

[86] *Id.*

[87] *See* Deanna Lambert, *County Sees Increase in Kids' Prank 911 Calls*, WSMV-TV (Dec. 31, 2009, 10:31 PM), http://www.wsmv.com/news/22094768/

Moreover, some jurisdictions have a policy that police must investigate every serious call placed to 911,[88] and some jurisdictions treat every call received as an emergency.[89] Anytime the police respond to an emergency, first responders race to reach the scene as quickly as possible, placing the lives of those in the community, as well as the responders themselves, in danger.[90]

iii. Harassment

Many commercial caller ID spoofing companies claim they are intended for entertainment via prank calls to friends, but the service is often used to prank call strangers or make threatening and demeaning calls to enemies.[91] Caller ID spoofing can aid harassers and stalkers by tricking a victim into answering a call.[92] In 2009, for example, a man called three women in the middle of the night claiming that he was inside their houses watching them.[93] He called the women's cell phones and spoofed their home numbers so that his victims believed he was calling from within

---

detail.html.

[88] *Id.*

[89] *See* Hailee Lampert, *Two Charged After Prank 911 Calls*, WLKY.COM (Feb. 26, 2010, 7:50 AM), http://www.wlky.com/r/22677032/detail.html.

[90] *I-Team: Prank 911 Calls Endanger Residents, Police*, WBALTV.COM (July 30, 2009, 8:25 AM), http://www.wbaltv.com/r/20214644/detail.html. A Baltimore policeman stated, "[e]very time we drive lights-and-siren, that raises the potential of harm to the officers themselves and other motorists on the road, for accidents. It poses a very significant risk to public safety." *Id.* In Texas, a fire engine, worth an estimated $450,000, flipped over while responding to a prank 911 call, injuring four firefighters. Michael N. Marcus, *911 Prank Call Injures Four Firefighters*, 911 WACKOS (Feb. 3, 2008, 5:31 AM), http://911wackos.blogspot.com/2008/02/911-prank-call-injures-four.html.

[91] *See* PHONEGANGSTER.COM, http://www.phonegangster.com/ (last visited Feb. 4, 2011) (claiming their services are intended for "fun"); *see also Real Stories/Uses*, SPOOFCARD, http://www.spoofcard.com/stories (last visited Feb. 4, 2011) (advertising testimonials from satisfied customers who were able to use the service to trick their friends).

[92] *Sabin Statement*, *supra* note 61.

[93] *Women Terrorized by Calls Appearing to Come From Home*, NBC PHILA. (Dec. 17, 2008, 7:45 AM), http://www.nbcphiladelphia.com/news/local-beat/Women-Terrorized-By-Calls-Appearing-To-Come-From-Home.html.

the house.[94]

iv. Political Harassment

Legitimate political "robocalling" is "one of the most-used political campaign tools."[95] However, Congress is concerned about the increasing use of political robocalls made with the intent to trick voters or prevent them from voting.[96] Caller ID spoofing is abused to make it appear that one candidate is placing a phone call, when in fact his opponent is using the call to annoy or confuse voters.[97] This happened to democrat Scott Kleeb, who ran to represent the 3rd District of Nebraska in the U.S. House of Representatives in 2006.[98] Automated calls were placed with spoofed caller ID information, making it look as if Kleeb's campaign placed the phone calls.[99] Voters received the calls overnight and sometimes repeatedly.[100] Mr. Kleeb is not the lone victim of this strategy. In South Carolina, police arrested a local Republican for purportedly organizing spoofed political robocalls.[101] Spoofing made the calls appear to be from the democratic candidate's office.[102]

---

[94] *Id.*

[95] Jason C. Miller, Note, *Regulating Robocalls: Are Automated Calls the Sound of, or a Threat to, Democracy?*, 16 MICH. TELECOMM. & TECH. L. REV. 213, 215 (2009).

[96] 153 CONG. REC. E1286 (daily ed. June 13, 2007) (statement of Rep. Green). Automated phone call devices can place as many as 100,000 calls in one hour. Miller, *supra* note 95, at 215. One automated phone call company reports they are able to call "10 to 20 percent of the U.S. population on a single day." *Id.* at 216.

[97] *Spoofer Calls Don't Leave Folks Laughing*, LINCOLN J. STAR, June 11, 2007, http://journalstar.com/news/opinion/editorial/article_3ce5eb06-803355b4-8151-be15654b2315.html.

[98] *Id*.

[99] *Id*.

[100] *Id.*

[101] Karen Daily, *Charges Brought in Robocall Case*, AIKEN STANDARD, Dec. 16, 2008, http://www.aikenstandard.com/local/1216Allen.

[102] *Id.* The woman was charged with unlawful use of a telephone under state law. *Id.*

There is anecdotal evidence that spoofed robocalls are effective at motivating voters to change their vote.[103] For example, in New Hampshire, the National Republican Congressional Committee placed repetitive robocalls, late at night, designed to appear to be from the democratic candidate.[104] The local newspaper printed a letter from an angry voter who stated she would not vote for the democratic candidate due to the annoying calls.[105]

III. STATE AND FEDERAL LEGISLATIVE APPROACHES

Increased concern over the damage caused by illegitimate uses of caller ID spoofing technology has triggered legislative responses at both the state and the federal level.[106] Four states have passed anti-spoofing legislation.[107] Congress considered six different versions of the Truth in Caller ID Act and three different versions of the Preventing Harassment Through Outbound Number Enforcement Act since 2006.[108] This section discusses the viability of the states' approaches to anti-spoofing legislation and introduces the federal legislation.

---

[103] Miller, *supra* note 95, at 221.

[104] *Id.* These calls did not use caller ID spoofing; rather, it was the content of the calls that was misleading. *Id*.

[105] *Id*.

[106] 156 CONG. REC. H2522, H2523 (daily ed. Apr. 14, 2010) (statement of Rep. Boucher); 152 CONG. REC. S3422, S3423 (daily ed. Apr. 24, 2006) (statement of Sen. Bill Nelson).

[107] Louisiana, Mississippi, Florida, and Oklahoma have passed anti-spoofing legislation. *See infra* Part III.A.

[108] Truth in Caller ID Act of 2010, H.R. 1258, 111th Cong. (2010); Truth in Caller ID Act of 2009, S. 30, 111th Cong. (2009); Preventing Harassment Through Outbound Number Enforcement Act of 2009, H.R. 1110, 111th Cong. (2009); Truth in Caller ID Act of 2007, S. 704, 110th Cong. (2008); Preventing Harassment Through Outbound Number Enforcement Act of 2007, H.R. 740, 110th Cong. (2007); Truth in Caller ID Act of 2007, H.R. 251, 110th Cong. (2007); Truth in Caller ID Act of 2006, S. 2630, 109th Cong. (2006); Preventing Harassment Through Outbound Number Enforcement Act, H.R. 5304, 109th Cong. (2006); Truth in Caller ID Act of 2006, H.R. 5126, 109th Cong. (2006).

A. State Legislation

Several states have proposed or enacted anti-spoofing legislation.[109] Louisiana's anti-spoofing bill provides a private right of action and enables the district attorney to "recover a civil penalty"[110] when "a caller . . . knowingly insert(s) false information into a caller identification system with the intent to mislead, defraud or deceive the recipient of a call."[111] Oklahoma's Anti-Caller ID Spoofing Act and Mississippi's Caller ID Anti-Spoofing Act also outlaw the knowing falsification of caller ID information to mislead, defraud or deceive.[112] In October 2008, Florida enacted the Caller ID Anti-Spoofing Act ("the Florida Act"), which outlawed spoofing to "deceive, defraud, or mislead."[113] By using the term "mislead," these statutes have the practical effect of outlawing all caller ID spoofing and rejecting the concept of legitimate uses.[114] Since the essence of caller ID spoofing is the ability to mislead called parties about the originating phone number, all uses become illegal under these statutes.[115]

In 2008, Teltech Systems, Inc.[116] filed a complaint alleging, among other things, that the Florida Act violated the Commerce Clause.[117] The Southern District of Florida agreed and granted

---

[109] Stolar & Gall, *supra* note 12.

[110] LA. REV. STAT. ANN. § 51:1741.5 (West 2010).

[111] *Id.* § 51:1741.4.

[112] MISS. CODE ANN. § 77-3-805 (West 2010); OKL. STAT. tit. 15, § 776.23 (West 2010). In 2009, Idaho considered, but ultimately did not enact, a similar anti-spoofing bill. Anti-Caller ID Spoofing Act, S. 1051, 60th Leg., Reg. Sess. (Idaho 2009), http://www.legislature.idaho.gov/legislation/2009/S1051.pdf.

[113] FLA. STAT. § 817.487 (West 2010).

[114] Plaintiff's Statement of Material Facts in Support of Motion for Summary Judgment, *supra* note 49, at 2.

[115] *Id.*

[116] *See supra* note 48 (discussing Teltech).

[117] Plaintiff's Memorandum of Law in Support of Motion for Summary Judgment at 17–19 Teltech Sys., Inc. v. McCollum, No. 08-61664-CIV-Martinez-Brown (S.D. Fla. July 16, 2009) (citing Pike v. Bruce Church, 397 U.S. 137 (1970)).

Teltech's motion for summary judgment.[118] Teltech argued that because of cellular phones and VoIP services, it could not know the location of the called parties.[119] For example, if a Teltech client in New York spoofed a call to a California number, the called party could be in fact located in Florida, rendering the New York client liable under the Florida Act.[120] Thus, Teltech argued it could not conduct its business in any state without fear of violating the Florida Act.[121] The court concluded that the Florida Act had "the practical effect of regulating commerce that occurs wholly outside the state of Florida" in violation of the Commerce Clause.[122]

Notwithstanding *Teltech*, states have continued to pass legislation similar to the Florida Act.[123] It is likely these statutes will be challenged in federal court,[124] but the outcome is unclear. In 2005, the U.S. Supreme Court denied certiorari on an appeal from a Washington state court ruling that a Washington anti-email spoofing statute, similar in effect to the Florida act, *did not* violate the Commerce Clause.[125] The Florida court did not find this persuasive in *Teltech*, but other Districts might.[126] The constitutional uncertainty of the existing state anti-spoofing

---

[118] *See Teltech*, No. 08-61664-CIV-Martinez-Brown.

[119] Plaintiff's Statement of Material Facts in Support of Motion for Summary Judgment, *supra* note 49, at 4. Likewise, simply blocking Florida area codes would not be sufficient to guarantee that no calls went into or originated in Florida. *Id.* at 5.

[120] *Teltech*, No. 08-61664-CIV-Martinez-Brown, at 16.

[121] *Id.*

[122] *Id.*

[123] *See* LA. REV. STAT. ANN. § 51:1741.4 (West 2010); MISS. CODE ANN. § 77-3-805 (West 2010).

[124] E-mail from Mark Del Bianco, Counsel, Teltech Sys., Inc., to author (Nov. 30, 2010, 10:04 AM) (on file with author). In November of 2010, Teltech filed a constitutional challenge to the Mississippi Caller ID Anti-Spoofing Act in the Southern District of Mississippi. *Id.*

[125] Heckel v. Washington, 24 P.3d 404 (Wash. 2001), *cert. denied*, 534 U.S. 997 (2001).

[126] *See Teltech*, No. 08-61664-CIV-Martinez-Brown; *see generally* Defendant's Response in Opposition to Plaintiff's Motion for Preliminary Injunction at 5 *Teltech*, No. 08-61664-CIV-Martinez-Brown, 2009 WL 1614869.

statutes, in addition to the small number of states that have enacted legislation, indicate that uniform and comprehensive regulation of caller ID spoofing must be accomplished at the federal level.

B. Federal Legislation

1. The Truth in Caller ID Act of 2009

On April 6, 2006, the long journey of the Truth in Caller ID Acts began.[127] Despite six attempts to pass this legislation, three in the House and three in the Senate,[128] the TICIDA did not pass both chambers until December 15, 2010.[129] On December 22, 2010, President Barack Obama signed the bill and it became Public Law 111-331.[130] The TICIDA amends section 227 of the Communications Act of 1934 ("the Act"), Title 47 of the U.S. Code, to outlaw certain uses of caller ID spoofing.[131]

The TICIDA forbids any person "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 . . . ."[132] Caller ID service is defined 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 IP-enabled voice service."[133]

---

[127] Truth in Caller ID Act of 2006, H.R. 5126, 109th Cong. (2006).

[128] Truth in Caller ID Act of 2010, H.R. 1258, 111th Cong. (2010); Truth in Caller ID Act of 2009, S. 30, 111th Cong. (2009); Truth in Caller ID Act of 2007, S. 704, 110th Cong. (2008); Truth in Caller ID Act of 2007, H.R. 251, 110th Cong. (2007); Truth in Caller ID Act of 2006, H.R. 5126, 109th Cong (2006); Truth in Caller ID Act of 2006, S. 2630, 109th Cong. (2006).

[129] *Id.*

[130] Library of Congress, *Bill Summary & Status*, THOMAS, http://www.thomas.gov/cgi-bin/bdquery/z?d111:s.00030: (last visited Feb. 4, 2011).

[131] S. 30.

[132] Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227(e)(1) (West 2010).

[133] § 227(e)(8)(B). Accordingly, the TICIDA regulates VoIP calls, as well as traditional phone calls. § 227(e)(1).

Generally, a willful and knowing initial violation of the Act is punishable by "a fine of not more than $10,000 or imprisonment for a term not exceeding one year, or both . . . ."[134] A second offense is punishable "by a fine of not more than $10,000 or by imprisonment for a term not exceeding two years, or both."[135] The TICIDA provides the FCC with enforcement power;[136] however, if the FCC determines that criminal prosecution is warranted, then it shall notify the United States Attorney, who shall bring the appropriate charges in the proper court.[137] Within six months, the FCC is to "prescribe regulations to implement" the TICIDA's provisions[138] 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 or IP-enabled voice service."[139]

The TICIDA provides specific civil and criminal penalties.[140] A specific civil forfeiture penalty, in addition to the general penalty under the Act, is "not to exceed $10,000 for each violation, or three times that amount for each day of continuing violation . . . ."[141] In contrast, a specific criminal fine under the TICIDA, of "not more than $10,000 for each violation, or three times that amount for each day of continuing violation," is "in lieu" of the general fines imposed under the Act.[142] However, the general criminal penalties under the Act, of imprisonment or a penalty of both fine and imprisonment, may be imposed in addition to the specific criminal fine.[143] Lastly, the TICIDA authorizes independent state enforcement via civil action in federal district

---

[134] Communications Act of 1934, 47 U.S.C.A. § 501 (West 2010).

[135] *Id.*

[136] § 227(e)(3)(A).

[137] Communications Act of 1934, 47 U.S.C.A. § 401 (West 2010).

[138] § 227(e)(3)(A).

[139] § 227(e)(4).

[140] *See* § 227(e)(5).

[141] § 227(e)(5)(A).

[142] § 227(e)(5)(B). Criminal penalties are imposed for "willful and knowing violation" of the TICIDA. *Id.*

[143] *Id.*

court.[144] After the FCC receives notice of the proceeding, it may, however, intervene in the state action.[145]

2. Past Proposals for Federal Legislation

The Preventing Harassment through Outbound Number Enforcement Act ("PHONE Act") was an alternative approach to caller ID spoofing regulation proposed in the House.[146] There have been three House versions of the PHONE Act, of which the first was introduced in 2006.[147] The most recent version, the PHONE Act of 2009, passed the House on December 16, 2009, with a resounding 418 "yeas" to one "nay,"[148] yet the bill died in the Senate.[149] Unlike the TICIDA, which amends Title 47 of the U.S. Code, the PHONE Act would have amended Title 18 by adding section 1041, "Caller ID Spoofing."[150] Section 1041(a) proposed to outlaw:

---

[144] § 227(e)(6)(A). The TICIDA provides:

> [t]he chief legal officer of a State, or any other State officer authorized by law to bring actions on behalf of the residents of a State, may bring a civil action, as parens patriae, on behalf of the residents of the State in the appropriate district court . . . to impose the civil penalties for violation of this subsection.

Id.

[145] § 227(e)(6)(C).

[146] Preventing Harassment Through Outbound Number Enforcement Act of 2009, H.R. 1110, 111th Cong. (2009). The most recent version, the PHONE Act, passed the House on December 16, 2009. Library of Congress, *Bill Summary & Status*, THOMAS, http://www.thomas.gov/cgi-bin/bdquery/D?d111:2:./temp/~bdq2yI::|/home/LegislativeData.php?n=BSS;c=111|, (last visited Feb. 4, 2011). There have been three House versions of the PHONE Act, of which the first was introduced in 2006. H.R. 1110; Preventing Harassment Through Outbound Number Enforcement Act of 2007, H.R. 740, 110th Cong. (2007); Preventing Harassment Through Outbound Number Enforcement Act, H.R. 5304, 109th Cong. (2006).

[147] H.R. 1110; H.R. 740; H.R. 5304.

[148] Library of Congress, *Bill Summary & Status*, THOMAS, http://www.thomas.gov/cgi-bin/bdquery/D?d111:2:./temp/~bdq2yI::|/home/LegislativeData.php?n=BSS;c=111|, (last visited Feb. 4, 2011).

[149] *Id.*

[150] H.R. 1110.

> knowingly [using] or [providing] to another (1) false caller ID information with intent wrongfully to obtain anything of value; or (2) caller ID information pertaining to an actual person or other entity without that person's or entity's consent and with intent to deceive any person or other entity about the identity of the caller . . . .[151]

A violation of subsection (a)(1) would have been punishable by a "[fine] under this title or imprison[ment] not more than 5 years, or both . . . ."[152] A violation of subsection (a)(2) would have been punishable by the same terms but with a one year maximum term of imprisonment.[153] In addition, any person convicted under section 1041 would have been subject to forfeiture of "(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and (B) any equipment, software or other technology used or intended to be used to commit or to facilitate the commission of such offense . . . ."[154]

IV. THE TRUTH IN CALLER ID ACT OF 2009 DOES NOT SOLVE THE PROBLEMS ASSOCIATED WITH ILLEGITIMATE CALLER ID SPOOFING

Although the TICIDA specifically outlaws illegitimate uses of caller ID spoofing, such legislation does not sufficiently respond to the issues caused by the continued availability of the technology. The TICIDA's weaknesses will encourage illegitimate users, thus undermining those who seek to use caller ID spoofing for valid purposes. Further response is necessary because caller ID spoofing provides valuable and legitimate services to society that ought to be preserved, as Congress repeatedly recognized during floor debates on the TICIDA.[155]

---

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] H.R. 1110 §§ (d)(1)(A)–(B).

[155] *See, e.g.*, 156 CONG. REC. H8378 (daily ed. Dec 15, 2010) (statement of Rep. Engel) ("I introduced the bill [inter alia] to protect legitimate uses of caller ID technology."); 156 CONG. REC. H2522 (daily ed. Apr. 14, 2010); *Cerasale Statement*, *supra* note 46; 152 CONG. REC. H9192, H9193 (daily ed. Dec. 8, 2006) (statement of Rep. Scott).

For many legitimate users, caller ID spoofing is the best way to keep caller ID private since the development of two new services has severely limited the effectiveness of *67 blocking.[156] One of these services is anonymous call rejection.[157] This service intercepts incoming calls from blocked or private numbers, which prevents the phone from ringing and instead notifies the caller that the number dialed does not receive anonymous calls.[158] This is problematic for domestic violence shelters and victims because courts sometimes order domestic violence victims to maintain contact with their ex-spouse to facilitate child custody arraignments.[159] If an abuser utilizes anonymous call rejection, caller ID spoofing becomes an indispensible tool for ensuring contact while protecting the location of the victim.[160]

The second new service is TrapCall.[161] This controversial service reveals blocked phone numbers, which raises privacy concerns for legitimate users.[162] When a TrapCall subscriber receives a blocked call, he can reject it.[163] TrapCall then re-routes the incoming call to an 800 number, revealing the caller's ANI.[164] The call is then sent back to the TrapCall subscriber's mobile phone with the private number displayed on the subscriber's caller

---

[156] *Knight Statement*, *supra* note 26, at 23.

[157] *Id.*

[158] *Fact Sheet 19: Caller ID and My Privacy*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/fs/fs19-cid.htm#18 (last visited Feb. 4, 2011).

[159] Elizabeth Olson, *A Technological Boost to the Cat-and-Mouse Game Between Callers and the Called*, N.Y. TIMES, Mar. 14, 2009, http://www.nytimes.com/2009/03/15/us/15call.html?_r=2.

[160] S. REP. NO. 110-234, at 2 (2007).

[161] Olson, *supra* note 159. Teltech launched TrapCall in 2009. *Id.* The service is currently available to AT&T, Verizon Wireless, Sprint, and T-Mobile subscribers as a free download. *Frequently Asked Questions*, TRAPCALL, http://www.trapcall.com/faq (last visited Feb. 4, 2011).

[162] Olson, *supra* note 159. It is argued that the service increases privacy and prevents harassment by allowing individuals to know the identity of callers. *Id.*

[163] *Id.*

[164] *Id.* While the call is re-routed, the caller continues to hear normal ringing. *Id.* See *supra* Part II.A for an explanation of ANI.

ID.[165] Caller ID spoofing is the only way to prevent TrapCall from revealing a private number since spoofing alters both the CPN and the ANI, protecting the private caller's information.[166]

Notwithstanding the important privacy gains caller ID spoofing provides, the grave personal and public costs of illegitimate uses require a comprehensive federal response. The TICIDA fails to provide this.[167] Unfortunately, if the TICIDA fails to curb illegitimate uses, Congress might decide to amend the TICIDA to adopt the states' approach of caller ID regulation, banning the technology outright.

In order to cure the deficiencies of the TICIDA and maintain the viability of caller ID spoofing, the Department of Justice, Congress, and the FCC should take a number of additional steps. First, federal prosecutors should creatively prosecute illegitimate users by charging the spoofer with the federal crime that best fits the illegitimate activities and provides the highest level of deterrence. Second, the FCC should notify Congress that text message caller ID spoofing will become a successor technology if Congress does not amend the TICIDA to define the term "call" as voice *and* text calls. Last, the FCC should enact regulations to facilitate law enforcement tracing of spoofed calls and create a Do-Not-Spoof list.

A. The Department of Justice Should Use Creative Prosecution Methods to Enhance Deterrence

During floor debates on the TICIDA, Congress members complained that spoofers could use the service legally to realize illegitimate ends.[168] Thus, it was argued, the TICIDA's criminal proscriptions were necessary to close that gap.[169] While the TICIDA now provides a direct method for federal prosecution of caller ID spoofing with the intent to "defraud, cause harm, or

---

[165] Olson, *supra* note 159.

[166] *Id.*

[167] *See* Part II.B.2 (explaining illegitimate uses).

[168] *See generally* 155 CONG. REC. S170, S173 (daily ed. Jan. 7, 2009) (statement of Mr. Nelson) (stating that many believe that this service is legal).

[169] *Id.* at S173–174.

wrongfully obtain anything of value,"[170] illegitimate caller ID spoofing was potentially prosecutable under numerous federal laws that provided steeper penalties than the TICIDA. The widespread use of caller ID spoofing technology for illegitimate ends suggests that effective deterrence requires vigorous and creative prosecution, which seeks to enhance the potential criminal penalties that illegitimate users face. Consequently, while prosecutors should charge those who use caller ID spoofing for swatting or political harassment under the TICIDA, for other illegitimate uses, it will be more effective to charge a spoofer under alternative federal statutes. The remainder of this section suggests which laws prosecutors should use when seeking to deter illegitimate users of caller ID spoofing, and the specific contexts in which these laws should be used.

1. Fraud Prosecution Methods

Committing fraud is generally illegal under many federal statutes that carry longer maximum penalties and larger maximum fines than the TICIDA, and those statutes should be used instead of the TICIDA to prosecute spoofing when appropriate.[171] The facts of the fraudulent scheme will determine which federal law applies.[172]

If the spoofer perpetrated fraud on a bank or financial institution, then the spoofer should be prosecuted under 18 U.S.C. § 1344, making him subject to "a fine of not more than $100,000, imprison[ment] of not more than 30 years, or both."[173] Otherwise, the spoofer should be prosecuted under 18 U.S.C. § 1343, which covers wire fraud generally.[174] Section 1343 provides that a party who "devises a scheme or artifice to defraud, or for obtaining money or property . . . by means of wire . . . shall be fined under

---

[170] Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227(e)(1) (West 2010).

[171] *See generally* Credit Card Fraud Act of 1984, 18 U.S.C.A. § 1029 (West 2010); Communications Act Amendments, 1952, 18 U.S.C.A. §§ 1343, 1344 (West 2010).

[172] *See generally* §§ 1029, 1343, 1344.

[173] § 1344.

[174] § 1343.

this title or imprisoned not more than 20 years, or both."[175]

While § 1343 should be used to prosecute interstate phishing schemes accomplished by spoofing,[176] by its terms, it applies only to "communication in interstate or foreign commerce . . . ."[177] Furthermore, some courts have held that where all parties are residents of the same state, "all telephone calls are *presumed to be intrastate* and, absent any indication otherwise . . . wire fraud is not [present]."[178] The TICIDA avoids this loophole since it does not have an interstate activity requirement.[179] Yet, the maximum penalty under the TICIDA is drastically lower than the maximum penalty under § 1343, thus providing a windfull to the intrastate spoofer charged under the TICIDA. Consequently, intrastate spoofers should be charged under state wire fraud and identity theft statutes[180] that have higher maximum penalties when available.

If the spoofer used caller ID information as an access device to commit fraud, the spoofer should be prosecuted under 18 U.S.C. § 1029.[181] Section 1029(a)(1) makes it illegal to "knowingly and with intent to defraud produce, use, or traffic in one or more counterfeit access devices."[182] An access device is defined as any

---

[175] *Id.*

[176] Black's law dictionary defines a "scheme" as "[a]n artful plot or plan, [usually] to deceive others." BLACK'S LAW DICTIONARY (9th ed. 2009).

[177] Communications Act Amendments, 1952, 18 U.S.C.A. § 1343 (West 2010). In addition, "money or property [must] be the object of the defendant's scheme to defraud." United States v. Martin, 411 F. Supp. 2d 370, 373 (S.D.N.Y. 2006). It is therefore possible that § 1343 does not include schemes to obtain personal information. Lastly, to be liable under § 1343, the use of the wires "must at least be 'incident to an essential part of the scheme.'" *Id*. at 374 (quoting United States v. Altman, 48 F.3d 96, 102 (2d Cir. 1995) (emphasis omitted)).

[178] Mathon v. Feldstein, 303 F. Supp. 2d 317, 324 (E.D.N.Y. 2004) (quoting McCoy v. Goldberg, 748 F. Supp. 146, 154 (S.D.N.Y. 1990)) (emphasis added).

[179] Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227 (West 2010).

[180] Christine Mumford, *Spam Gives Way to Data Breach, Phishing in Contest for State Legislators' Attention*, 8 COMPUTER TECH. L. REP. (BNA) 56 (Feb. 2, 2007).

[181] Credit Card Fraud Act of 1984, 18 U.S.C.A. § 1029 (West 2010).

[182] § 1029(a)(1).

"code, account number, . . . mobile identification number, personal identification number, . . . or other means of account access that can be used . . . to obtain money, goods, services, or any other thing of value . . . ."[183] Caller ID information is a unique number that the spoofer uses to obtain things of value in phishing schemes and in false identity verifications.[184] In a phishing scheme, the spoofer uses caller ID to access personal information, which the spoofer can sell or use to obtain goods or cash.[185] When it fraudulently verifies identity, caller ID is an account number that leads directly to the spoofer obtaining money, or valuable confidential information.[186] Thus, § 1029 should be charged when phishers spoof false caller ID numbers to obtain things of value.

Alternatively, if the phisher pretends to be a trusted entity, he can be prosecuted according to the mask he wears or the identity of his victims. Those who falsely assume the identity of a government official should be prosecuted under 18 U.S.C. § 912, which carries a criminal penalty of up to three years imprisonment.[187] If caller ID spoofing is used in connection with a fraudulent telemarketing scheme, the spoofer should be prosecuted under 18 U.S.C. § 2326, which would subject him to an enhanced penalty of up to five years imprisonment.[188] If during that scheme he victimized "ten or more persons over the age of 55; or targeted persons over the age of 55," § 2326 provides "imprison[ment] for a term of up to 10

---

[183] § 1029(e)(1).

[184] *See* Plaintiff's Statement of Material Facts in Support of Motion for Summary Judgment, *supra* note 49, at 2 (noting that the government had admitted "that on a telephone call the Caller ID string is akin to the identity of the caller").

[185] RAYSMAN & BROWN, *supra* note 63.

[186] *See* S. REP. NO. 110-234, at 2 (2007).

[187] Major Crimes Act, 18 U.S.C.A. § 912 (West 2010).

> Whoever falsely assumes or pretends to be an officer or employee acting under the authority of the United States or any department, agency or officer thereof, and . . . in such pretended character demands or obtains any money, paper, document, or thing of value, shall be fined under this title or imprisoned not more than three years, or both.

Id.

[188] Senior Citizens Against Marketing Scams Act of 1994, 18 U.S.C.A. § 2326(1) (West 2010).

years."[189]

Finally, voicemail hacking is prosecutable under either the Stored Communications Act[190] or the Wiretap Act[191] depending on the actions taken by the spoofer once he accesses the voicemail system.[192] If the spoofer merely accesses the system, then he should be prosecuted under the Stored Communications Act, which provides a maximum penalty of five years in prison.[193] If however the spoofer also records copies of messages or deletes messages from the system, he has then intercepted communications and should be prosecuted under the Wiretap Act, which provides for penalties of up to five years in prison.[194]

2. Swatting Prosecution Methods

The TICIDA is the most effective method of prosecuting swatting. Before the TICIDA, there was no federal statute that outlawed spoofed 911 calls.[195] However, certain states had

---

[189] Senior Citizens Against Marketing Scams Act of 1994, 18 U.S.C.A. § 2326(2) (West 2010). A Minnesota report stated that caller ID spoofing "provide[d] convincing support to criminals" in a fraudulent telemarketing lottery scheme. MINN. PUB. UTIL. COMM'N, STAFF BRIEFING PAPER, Docket No. P=999/C-08-1391, 1 (2010).

[190] Electronic Communications Privacy Act of 1986, 18 U.S.C.A. § 2701 makes it illegal to "intentionally access without authorization a facility through which an electronic communication service is provided" and "thereby [obtain], [alter], or [prevent] authorized access to a wire or electronic communication." § 2701(a).

[191] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. § 2511, outlaws the interception and disclosure of wire, oral, or electronic communications. The section provides that any person who "intentionally intercepts, . . . any wire, oral, or electronic communication . . . shall be fined under this title or imprisoned not more than five years, or both." *Id.*

[192] United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998) (discussing the complexity of both acts and determining that the best approach is one that determines their applicability based upon whether the defendant merely accesses the system or accesses and records or intercepts messages from the system).

[193] *Id.*; § 2701(b)(1).

[194] *Smith*, 155 F.3d at 1058; § 2511(4)(a).

[195] *See generally* Rana Sampson, *Guide 19: Misuse and Abuse of 911*, PROBLEM ORIENTED GUIDES FOR POLICE 13 (U.S. Dep't of Justice, Office of

promulgated statutes that specifically outlawed fake, false, or fraudulent 911 calls.[196] For example, in Oklahoma and Georgia, false 911 calls are first-degree misdemeanors.[197] Rhode Island imposes a maximum fine of $1,000 dollars and/or a maximum sentence of one-year imprisonment for knowingly making false reports to emergency services.[198] The offense became a felony in Illinois in response to public outcry after a police officer's car flipped over as he sped to the scene of a false 911 report of five dead bodies.[199] However, the monetary penalties under the TICIDA are considerably higher than under state laws. Consequently, prosecutors should charge swatters under the TICIDA.

3. Harassment Prosecution Methods

Congress first enacted legislation on annoying or harassing phone calls in 1968.[200] These and other federal statutes provide more stringent penalties than the TICIDA, and consequently

---

Cmty. Oriented Policing Servs. Ser. No. 19, 2004), Aug. 2004, *available at* http://www.cops.usdoj.gov/files/ric/Publications/e07042423_web.pdf.

[196] There are also non-specific statutes under which swatters may be prosecuted. Alexis Stevens, *7th Graders Arrested After 911 Prank Calls*, ATLANTA J.-CONST., Mar. 24, 2010, http://www.ajc.com/news/cobb/7th-graders-arrested-after-401061.html. For example, two juveniles were charged with "transmission of false public alarm and disruption of a public school" after making prank 911 calls on school grounds. *Id.* In New York, a teenager was charged with disorderly conduct after placing prank 911 calls. Ben Muessig, *Teen Who Made Prank 911 Call Has History of False Reports*, GOTHAMIST (March 1, 2010, 4:57 PM), http://gothamist.com/2010/03/01/teen_who_made_prank_911_call_has_hi.php. Lastly, a Kentucky man was charged with wanton endangerment for making a false 911 calls. Lampert, *supra* note 89.

[197] GA. CODE ANN. § 16-11-39.2(b) (West 2010); OKLA. STAT. tit. 63, § 2819 (West 2010).

[198] R.I. GEN. LAWS § 39-21.1-16 (West 2010).

[199] Monique Garcia, *Prank 911 Calls to Carry Stiffer Penalty*, CHI. TRIB., July 26, 2010, http://newsblogs.chicagotribune.com/clout_st/2010/07/prank-911-calls-to-carry-stiffer-penalty.html.

[200] SHARON K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE 290 (Rick Adams ed., 2002). Indeed, many states have also passed laws criminalizing harassment via intrastate phone calls. *Id.*

should be used to prosecute harassment when applicable. Title 47, § 223 of the U.S. Code prohibits "[o]bscene or harassing telephone calls" and violations thereunder are subject to a fine, imprisonment of up to two years, or both.[201] Section 223(a)(1)(C) prohibits the use of "a telecommunications device, whether or not conversation or communication ensues, without [the disclosure of the caller's] identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications."[202] In *United States v. Bowker*, the defendant was found guilty of telephone harassment under § 223(a)(1)(C) after he placed multiple unwanted calls using *67 to block his caller ID information.[203] The defendant argued, unsuccessfully, that even though the caller ID information was blocked, the victim could recognize his voice, which meant that his identity was not actually concealed.[204] The court held that the defendant had failed to disclose his real identity when he identified himself by another name during phone calls and voice messages.[205] Thus, anytime a spoofer uses the technology to harass, annoy, abuse, or threaten, and the spoofer does not state his name during the call, he should be prosecuted under this section.

Congress has also outlawed stalking via telephone calls.[206] Title 18, § 2261A(2) of the U.S. Code provides that whoever uses "any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to [his victim]" with intent to harass is punishable by up to five years

---

[201] Communications Act of 1934, 47 U.S.C.A. § 223(a)(1) (West 2010).

[202] § 223(a)(1)(C). In *United States v. Popa*, the U.S. Court of Appeals for the District of Columbia defined these terms: "To annoy means to irritate, to bother, to make someone angry by repeated action; to abuse means to use insulting, coarse or bad language about or to someone; . . . and, fourth, to harass means to trouble, to worry or torment." United States v. Popa, 187 F.3d 672, 674 (D.C. Cir. 1999).

[203] *See generally* United States v. Bowker, 372 F.3d 365 (6th Cir. 2004).

[204] *Id.* at 390.

[205] *Id.* (holding that a receiver's ability to "suspect, or have a very good idea of, the caller's identity" is irrelevant to the question of whether the defendant disclosed his identity).

[206] *See* Safe Homes for Women Act of 1994, 18 U.S.C.A. § 2261A(2) (West 2010).

imprisonment, a fine, or both.[207] In *Bowker*, the Sixth Circuit held that harassing and threatening telephone conversations and voicemail messages, coupled with the victim's testimony that these conversations and messages made her fearful of leaving her house, were sufficient to uphold a conviction under § 2261A.[208] Thus, a stalker who manipulates caller ID in order to gain access to his victim and causes her emotional distress should be prosecuted under § 2261A.

4. Political Harassment Prosecution Methods

The TICIDA should be charged in political harassment prosecutions rather than other available federal alternatives. Title 18 U.S.C. § 241 provides that "[i]f two or more persons conspire to injure, oppress, threaten, or intimidate any person . . . in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or law of the [United States] . . . [t]hey shall be fined under this title or imprisoned not more than ten years, or both . . . ."[209] This section requires a specific intent to violate the victim's constitutional rights; however, this intent need not be the sole intent of the conspiracy.[210] Nonetheless, it might be difficult to prove that robocalls that merely provided false information through benign language intimidated or oppressed the called party. In these circumstances, § 241 might not be effective in this context.

Alternatively, 42 U.S.C. § 1971(b) provides that "[n]o person, whether acting under color of law or otherwise, shall intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose . . . ."[211] Since political harassment is arguably an attempt to coerce voters, § 1971(b) seems like an easier fit in political harassment prosecutions than § 241. However, § 1971(b) does not provide for

---

[207] *Id.*

[208] *See Bowker*, 372 F.3d at 370.

[209] Major Crimes Act, 18 U.S.C.A. § 241 (West 2010).

[210] United States v. Ellis, 595 F.2d 154, 161–62 (3d Cir. 1979).

[211] Civil Rights Act of 1957, 42 U.S.C.A. § 1971(b) (West 2010).

criminal penalties.[212] Given the deficiencies of the available alternative methods of federal prosecution, the TICIDA should be utilized to prosecute political harassers who utilize caller ID spoofing.

B. The FCC Should Inform Congress that Text Message Spoofing Will Become a Successor Technology in its Section (e)(4) Report[213]

The TICIDA is underinclusive because it is unclear whether it also prohibits nefarious text message spoofing. Effective legislation must define "call" to include both voice and text calls. Text messages are "the most successful communications medium since e-mail,"[214] and almost 90 percent of Americans use a cell phone.[215] Text message spoofing can accomplish many of the same illegitimate ends as traditional caller ID spoofing, as well as other harms specific to the text message medium.[216] If the TICIDA does not expressly cover text message spoofing, then illegitimate users might simply spoof caller ID through different means. Accordingly, the FCC should notify Congress in its section (e)(4)

---

[212] § 1971(c). However, the Attorney General may seek a preventative injunction against any party for which there are reasonable grounds to anticipate a violation. *Id.*

[213] Section (e)(4) of the TICIDA provides that the FCC "shall 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 service or IP-enabled voice service." Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227(e)(4) (West 2010).

[214] Pieter Streicher, *SMS Is Not to blame*, ITWEB ONLINE, July 29, 2009, http://www.itweb.co.za/index.php?option=com_content&view=article&id=24866:sms-is-not-to-blame&catid=143&Itemid=99 ("[Text] messages can be sent to more than three billion people worldwide, and in 2008, a total of six trillion [text] messages were sent globally.").

[215] Press Release, Spoofem.com, Spoofem.com Uses Mobile Media for New Marketing Method (Aug. 4, 2010) (on file with author). In addition, "52,083 text messages are sent every second," with 83% being read within one hour of receipt. *Id.* Revenue from text messaging is estimated to reach $110 billion annually by 2013. Streicher, *supra* note 214.

[216] *SMS Spoofing*, WIKIPEDIA, http://en.wikipedia.org/wiki/SMS_spoofing (last visited Feb. 4, 2011).

report that text message spoofing will become a successor technology if it is not included under the TICIDA's prohibitions.

As with traditional caller ID spoofing, illegitimate users exploit text message caller ID spoofing to harass or defraud others.[217] For example, a Kansas court awarded $7.3 million in a harassment suit where the defendant sent the plaintiff and the plaintiff's family "profane and defamatory text messages" using a spoofing service to mask her identity.[218] When spoofers phish through text messages, it is known as "smishing."[219] In one common fraud, a spoofed text message informs victims that her bank account has been suspended.[220] The message states that the victim must call an 800 number in order to unlock her account.[221] Upon dialing this number, a message instructs the victim to enter her debit or credit card account number, pin, and expiration date.[222] There have also been reports of spoofed text messages that fool receivers into downloading costly programs.[223] In one scheme, a cell phone user receives a text message that reads, "Please call the hospital, it's your mother."[224] However, when the cell phone user calls the number in the text message, a call is placed to a premium rate service,[225] and the user inadvertently downloads a virus that sends

---

[217] Bill Meyer, *Spoofing Scams Make Caller ID Untrustworthy, Can Be Used to Defraud, Terrify Victims*, CLEVELAND.COM (Sept. 17, 2009, 1:29 PM), http://www.cleveland.com/nation/index.ssf/2009/09/spoofing_scams_make_caller_id.html.

[218] *Id.*

[219] *Smishing is a New Cyber Fraud That Uses SMS Messages*, NORTHERN STAR (Australia), Nov. 17, 2009, at 15.

[220] Brian Krebs, *Security Fix: The Anatomy of a Vishing Scam*, WASH. POST (Mar. 15, 2008, 5:54 PM), http://voices.washingtonpost.com/securityfix/2008/03/the_anatomy_of_a_vishing_scam_1.html; *see also Smishing is a New Cyber Fraud That Uses SMS Messages*, *supra* note 219.

[221] Krebs, *supra* note 220.

[222] *Id.*

[223] *See generally* Ed Finegold, *Internet-like Services Bring Internet-like Crime*, BILLING WORLD AND OSS TODAY, May 1, 2007, http://www.billingworld.com/articles/2007/05/internet-like-services-bring-internet-like-crime.aspx.

[224] *Id.*

[225] *Id.* Premium text messages enable cell users to purchase goods billed to

premium text messages without the user's knowledge.[226]

The TICIDA defines "caller identification service" 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 IP-enabled voice service."[227] Unfortunately, the TICIDA does not define the term "call."[228] Of course, it is possible that the FCC or the courts will interpret the TICIDA to include text calls.[229] Indeed, the FCC has interpreted the Telephone Consumer Protection Act ("TCPA") to include text messages even though the statute did not expressly cover text messages.[230] The TCPA prohibits any call placed to "any telephone number assigned to a paging service, cellular telephone service, . . . or any service for which the called party is charged" using an automatic dialing system or an artificial or prerecorded voice.[231] The FCC determined that the term "call" under the TCPA includes voice calls and text calls, reasoning that the distinguishing factor was not the type of call placed, but whether the call was placed to a telephone number assigned to a pay service.[232] Thus, if the FCC were to apply similar logic to the TICIDA, perhaps the FCC would find that the determinative factor is whether the caller ID information was spoofed, not whether the communication was made via voice or text call.

However, federal courts are not necessarily bound to incorporate the same interpretation as the FCC.[233] In determining whether to adopt an agency's interpretation of an ambiguous statute, a court utilizes a two-step process outlined by the Supreme Court in *Chevron, Inc v. Natural Resources Defense Council,*

---

the cell phone bill. *Id.*

[226] *Id.*

[227] Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227(e)(8) (West 2010).

[228] *See id.*

[229] *See generally* Implementing the Telephone Consumer Protection Act of 1991, 18 FCC Rcd. 14014, 14115 (2003).

[230] *See id.*

[231] *Id.*

[232] *See id.*

[233] Chevron, Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842 (1984).

Inc.[234] First, the court asks, "whether Congress has directly spoken to the precise question at issue."[235] Second, the court asks if the agency's interpretation is reasonable.[236] If these two questions are answered in the affirmative, "a court must defer to the federal agency's interpretation of the statute . . . ."[237] In *Satterfield v. Simon & Schuster, Inc.*, the Ninth Circuit adopted the FCC's interpretation of the term "call" under the TCPA.[238] In so holding, the court weighed heavily on Congress' delegation of authority to the FCC to implement the TCPA and the fact that "call" was undefined in the TCPA.[239] Noting that the TCPA was enacted before the availability of text message technology, the court held that Congress could not have clearly spoken about the TCPA's applicability to text calls.[240] Of course, text messages were available before the TICIDA's enactment, making Congress' omission appear more deliberate. Accordingly, even if the FCC were to interpret "call" to include text calls, thereby utilizing its authority to implement the statute, the issue would not simply be settled; courts would nonetheless apply the *Chevron* analysis before deciding whether to adopt the FCC's interpretation of the statute. This would render the legal status of text message spoofing under the TICIDA unclear once again.

Since text message spoofing can be used to accomplish that which the TICIDA clearly prohibits, the TICIDA must cover text message spoofing to prevent illegitimate spoofers from utilizing this successor technology. Therefore, the FCC should notify Congress in its section (e)(4) report that Congress must define the term "call" to include text message calls expressly.

---

234 *Id.*

235 *Id.*

236 *Id.*

237 Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 952 (9th Cir. 2009).

238 *Id.*

239 *Id.* at 953.

240 *Id.* at 954.

C. The FCC Should Pass Regulations to Facilitate Law Enforcement Tracing and to Create a Do-Not-Spoof List

During debates on the TICIDA and the PHONE Act, Congress members voiced concerns about law enforcement tracing and the unauthorized substitution of other individuals' phone numbers during spoofed calls.[241] The TICIDA does not directly address these concerns.[242] Before the passage of the TICIDA, the FCC stated that its jurisdiction over caller ID spoofing companies was unclear.[243] However, now that the TICIDA is law, the FCC must "pass regulations to implement [the TICIDA]."[244] On January 26, 2011, the Department of Justice requested that the FCC promulgate rules of this nature.[245] Moreover, the legislative history shows that Congress intended the FCC to pass regulations "imposing obligations on entities that provide caller ID spoofing services to the public."[246] This section argues that the FCC should promulgate regulations to address these concerns and any others necessary to maintain the viability of the industry.

1. Tracing

During congressional debates on the TICIDA and the PHONE Act, representatives expressed concern about the difficulty of

---

[241] Letter from Lanny A. Breuer, Assistant Atty. Gen., U.S. Dep't of Justice, to Marlene H. Dortch, Sec'y, Fed. Commc'ns Comm'n (Jan. 26, 2011), *available at* http://www.telecomlawmonitor.com/uploads/file/DOJ%20Truth%20in%20Caller%20ID%20letter.pdf.

[242] *Id.*

[243] *Monteith Statement*, *supra* note 51, at 3–4.

[244] Truth in Caller ID Act of 2009, 47 U.S.C.A. § 227(e)(3)(A) (West 2010).

[245] Letter from Lanny A. Breuer to Marlene H. Dortch, *supra* note 241, at 4 ("[T]he Commission should . . . allow law enforcement to trace such calls to the true originating telephone number with appropriate authority."); *id.* at 3 ("The Department of Justice shares Congress' concern about the ready availability of services that allow users to spoof telephone numbers with which they have no association whatsoever.").

[246] 156 CONG. REC. H8378 (daily ed. Dec 15, 2010) (statement of Rep. Boucher).

tracing spoofed calls.[247] When correct caller ID information is reported, civilians and law enforcement agencies are able to dial *57 to implement a tracing service that stores information about the caller for the use of law enforcement.[248] That technology does not render correct information when the number is spoofed, making the tracing process more time-consuming.[249]

Although tracing a spoofed call might be difficult, it is possible.[250] Often, tracking down the caller requires subpoenaing either the commercial spoofing company or the VoIP provider.[251] Teltech reports that it "take[s] a very proactive approach to help law enforcement" when its service is used illegally.[252] In order to help law enforcement trace spoofed phone calls, the FCC should promulgate record-keeping regulations applicable to commercial spoofing companies and VoIP providers. These regulations should specify what information must be kept by spoofing companies, the period of time such records must be kept, and the penalties that should be imposed for failure to keep such records.

2. Do-Not-Spoof List

Another concern voiced during the debates on the PHONE Act was the protection of those whose numbers are used to mask the identity of the spoofer.[253] Often a spoofer will substitute the same

---

[247] *Sabin Statement*, *supra* note 61 (discussing the difficulty police encountered when trying to locate the source of threatening spoofed phone calls made to a police officer and his family and expressing concern that spoofing could "complicate criminal investigations").

[248] *See Preventing Harassment Through Outbound Number Enforcement (PHONE) Act: Hearing on H.R. 5304 Before Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 109th Cong. 28 (2006) (statement of Rep. Murphy).

[249] *Id.*

[250] *See id.*

[251] *Id.*

[252] Meyer, *supra* note 217.

[253] *See generally Preventing Harassment Through Outbound Number Enforcement (PHONE) Act: Hearing on H.R. 5304 Before Subcomm. On Crime, Terrorism, and Homeland Security,* 109th Cong. (2006) [hereinafter *Kiko Statement*] (statement of Phil Kiko, Chief of Staff and General Counsel, U.S.

number repeatedly.[254] This happened to Phil Kiko, Chief of Staff and General Counsel to the House of Representatives, who received upwards of twenty phone calls per day from individuals who believed that he was repeatedly calling them.[255] Instead, a spoofer had placed those calls spoofing Mr. Kiko's name.[256] Currently, those whose numbers are used to spoof have few options but to change their phone numbers.[257]

Subsection two of the PHONE Act would have criminalized the use of "caller ID information pertaining to an actual person or other entity without that person's or entity's consent and with intent to deceive any person or other entity about the identity of the caller" in an apparent attempt to minimize unauthorized use of numbers.[258] However, it is too demanding to require that everyday users of caller ID spoofing technology determine whether a phone number belongs to another individual. Any such requirement would likely have negative effects on legitimate users, such as domestic violence victims, who might chose a random string of numbers without realizing it is in fact another's phone number. In addition, the threat of criminal sanction for failure to get approval to spoof a number will force these victims to use their relatives' or friends' phone numbers, which might reveal too much about their locations. Thus, the providers of caller ID spoofing should assume the responsibility for determining whether the use of a phone number is appropriate.

On January 26, 2011, the Department of Justice suggested that the FCC "should consider the feasibility of requiring public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number."[259] However, such a requirement is far too burdensome on the

---

House of Representatives).

[254] *Id.*

[255] *Id.*

[256] *Id.*

[257] *Id.*

[258] Preventing Harassment Through Outbound Number Enforcement Act of 2009, H.R. 1110 § (2), 111th Cong. (2009).

[259] Letter from Lanny A. Breuer, *supra* note 241, at 3.

industry. Just one public provider of caller ID spoofing services reported having over three million customers[260] and these customers might have substituted more than one number each. Clearly, implementing such a system, which placed a phone call to every proposed substitute number, would require a massive undertaking by public providers. Moreover, the system would be inefficient, as repetitive calls would surely occur.

Instead, the FCC should promulgate regulations mandating that commercial spoofing companies maintain a shared Do-Not-Spoof list. Unlike the Department of Justice's proposed method, this list would prevent spoofers from substituting the listed number or calling listed numbers with spoofed caller ID information. Additionally, all caller ID companies would share the price of maintaining such a list, preventing the duplicate costs incurred under the Department of Justice's proposed method.

Spoofing companies already maintain lists that operate in a similar manner. SpoofCard reports that it maintains a list of numbers that spoofers cannot call.[261] It created this list in an effort to prevent swatting and SpoofCard continually works to increase the list of police numbers that are not spoofable.[262] In addition, Spoofem.com now offers SpoofAbuse, where for five dollars one can provide up to three numbers which the company will put on its do not spoof list, so its customers will no longer be able to make spoofed calls to that number.[263] Spoofem.com also provides these numbers to other commercial spoofing companies; however, it does not guarantee that other companies will respect the subscriber's request.[264] Thus, the technology for a Do-Not-Spoof list exists, but could be used more efficiently.

Any Do-Not-Spoof list should include emergency and government numbers so customers cannot engage in swatting and so phishers cannot spoof these numbers to trick others. Individuals

---

[260] Thomas, *supra* note 29 (noting that the number one spoofing company, SpoofCard, has over three million customers).

[261] Meyer, *supra* note 217.

[262] *Id.*

[263] *SpoofAbuse*, SPOOFEM.COM, http://spoofem.com/spoofabuse (last visited Feb. 4, 2011).

[264] *Id.*

should be able to contact spoofing providers directly and the FCC should determine a method for phone service providers to report their customers' requests to be added to the list.[265] Lastly, the FCC should determine the appropriate sanctions to impose when companies fail to honor individuals' requests that their numbers not be used for spoofing.

V. CONCLUSION

Caller ID spoofing provides real societal benefits, but can also deliver dangerous blows.[266] The trust many place in their caller ID service gives spoofers an advantage when they commit crimes, but spoofing also provides necessary shelter to many legitimate users.[267] The Truth in Caller ID Act of 2009 is a step in the right direction; however, additional federal response is necessary. The Department of Justice should utilize its full array of options to prosecute creatively when appropriate, so that the charge conveys the gravity of the crime. In addition, the TICIDA must clearly include text message caller ID spoofing because it is used to accomplish the same illegitimate ends as traditional caller ID spoofing. Lastly, the FCC should promulgate regulations to help law enforcement trace illegitimate users and create a Do-Not-Spoof list. With a comprehensive approach, Congress will be able to ensure the legality of caller ID spoofing technology for legitimate users, while also minimizing illegitimate uses. Victims of caller ID spoofing, like Doug Bates, should feel safe in their homes again.

---

[265] *Monteith Statement*, *supra* note 51; s*ee also Kiko Statement*, *supra* note 253, at 23 (lamenting that his telephone provider informed him that he could not prevent spoofing accomplished with his phone number).

[266] *See supra* Part II.B (explaining legitimate and illegitimate uses of caller ID spoofing).

[267] 153 CONG. REC. H6257, H6258–59 (daily ed. June 12, 2007) (statement of Rep. Engel).