Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF THE NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Cindy Southworth
Vice President of Development & Innovation
2001 S St NW, Suite 400
Washington, DC 20009
phone: 202-543-5566
fax: 202-543-5626

Guilherme Roschke, Esq.
Angela Campbell, Esq.
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9535

Counsel for National Network to End Domestic Violence

Khaliah Barnes
Samuel Philipson

Law Students
Georgetown Law

April 18, 2011

SUMMARY

The National Network to End Domestic Violence (NNEDV) responds to the Commission's request for comments on its Notice of Proposed Rulemaking in the matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009. The Act prohibits the use of false or misleading caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless exempted.

First, NNEDV urges the Commission to adopt rules that clarify that organizations that use spoofing technology to protect victims of domestic violence, dating violence, sexual assault, or stalking are not violating the law. The Commission should therefore exempt any "Victim Service Provider," as defined in the Violence Against Women Act of 1994.

Second, NNEDV urges the Commission to define "harm" to include stalking, harassment, and the violation of protection and restraining orders. This inclusive definition will more clearly address the nefarious uses of caller ID spoofing. Caller ID spoofing harms should cover harassment and stalking because they cause substantial emotional distress and cause victims to fear for their safety or the safety of others. Violations of protection and restraining orders should also be considered "harm" because they protect victims from unwanted harassment and communications.

Third, because of the proliferation of third-party caller ID spoofing services that encourage nefarious spoofing, the Commission should require third-party caller ID spoofing services to give prominent notice that use of their services in violation of the Truth in Caller ID Act is unlawful. The service providers' small print legal disclaimers currently in place do not effectively inform spoofing users of permissible and impermissible caller ID spoofing.

Requiring third-party prominent notice of the legal ramifications of caller ID spoofing misuse should help to discourage impermissible caller ID spoofing.

Fourth, NNEDV further requests the Commission impose obligations on unmasking service providers to notify callers when their blocked caller ID will be unmasked and require affirmative opt-in consent before removing their privacy indicator. Companies that offer services to unmask blocked caller ID are potentially endangering victims by allowing their abusers to see their hidden phone numbers. Forwarding calls through a service such as TrapCall, which does not notify calling parties it is in operation, works against the intention of the original Calling Number Identification Service rulemaking. We ask the Commission to preserve consumers' expectation of the efficacy of caller ID blocking, requiring that third-party caller ID unmasking services provide callers with notice that the service is in place and give them the ability to "opt-in" to providing their caller ID to the call recipient.

Finally, the Commission should report to Congress on the potential for SMS and location spoofing. Both offer the same potential as caller ID spoofing – the ability of innocent parties to protect themselves and the ability of nefarious parties to cause harm.

TABLE OF CONTENTS

SUMMARY ..... **i**

COMMENTS OF NATIONAL NETWORK TO END DOMESTIC VIOLENCE **1**

I. THE COMMISSION SHOULD PROVIDE AN EXEMPTION TO ITS RULES TO PROTECT THE USE OF SPOOFING FOR LEGITIMATE SAFETY PURPOSES. *2*

II. THE COMMISSION SHOULD DEFINE "HARM" TO PROTECT VICTIMS *4*

III. THE COMMISSION SHOULD REQUIRE THIRD-PARTY CALLER ID SPOOFING SERVICES TO GIVE PROMINENT NOTICE THAT USE OF THEIR SERVICES IN VIOLATION OF THE TRUTH IN CALLER ID ACT IS UNLAWFUL. *8*

A. Existing Notices of Truth in Caller ID Act Violations are Inadequate and Contradictory 8

B. Requiring Third-Party Prominent Notice Of The Legal Ramifications Of Caller ID Spoofing Misuse Should Discourage Impermissible Caller ID Spoofing 14

IV. THE COMMISSION SHOULD REQUIRE CALLER ID UNMASKING SERVICES TO NOTIFY CALLERS, AND PROVIDE THEM WITH THE ABILITY TO "OPT-IN," WHEN THEIR PRIVACY INDICATOR IS BEING OVERRIDDEN. *17*

A. Congress and the Commission Have Long Recognized an Interest in Protecting a Calling Party's Privacy Indicator 19

B. Callers Should Be Provided Choice, in the Form of an Opt-In, When a Third Party Will Unmask Their Caller ID. 21

V. THE COMMISSION SHOULD INCLUDE AN ANALYSIS OF THE THREATS FOR SMS AND LOCATION SPOOFING IN ITS REPORT TO CONGRESS. *22*

CONCLUSION **24**

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF NATIONAL NETWORK TO END DOMESTIC VIOLENCE

The National Network to End Domestic Violence (NNEDV) is a not-for-profit network of fifty-six state and territory domestic violence coalitions, incorporated in the District of Columbia. NNEDV represents over 2,000 local domestic violence programs across the nation through its member coalitions. Through its Safety Net Project, NNEDV addresses privacy, databases, technology, and stalking. A first-of-its-kind endeavor, the Safety Net Project educates victims of domestic and sexual violence, their advocates and the general public on strategic ways to use technology to increase individuals' safety. Safety Net also assists law enforcement officials, judges, prosecutors and victim advocates on how to abusers misuse technology to further their abuse. The effect of caller ID “spoofing” and “unmasking” technology on victims is an example of Safety Net Project concerns.

Technological innovations have made it possible for average consumers to circumvent the caller ID system through spoofing IDs and unmasking blocked IDs. Spoofing is the practice of sending a caller ID signal from a false or alternate number when making a call, thereby tricking the receiving party into believing the call originated from someone other than the caller. This practice can be used for positive ends, such as disguising the identity and location of calls from a victim service provider to victims’

homes. It can also be used for malicious and nefarious ends. It is also possible for the average consumer to "unmask" blocked ID calls through services that strip away the caller's privacy indicator. Congress passed the Truth in Caller ID Act to address the danger of malicious caller ID spoofing, and directed the FCC to adopt rules addressing malicious caller ID spoofing and unmasking technologies.[1] In its Notice of Proposed Rulemaking (NPRM), the FCC has requested comments on the best means to address these new technologies.[2]

I. THE COMMISSION SHOULD PROVIDE AN EXEMPTION TO ITS RULES TO PROTECT THE USE OF SPOOFING FOR LEGITIMATE SAFETY PURPOSES.

The Act generally prohibits spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value. The Commission inquires about additional exemptions to implement.[3] To preserve the safety and privacy of victims of domestic violence, sexual assault, dating abuse, and stalking, we request the Commission include in its final rules an exemption from the requirements of proposed 47 C.F.R. § 64.1604(a) for victim service providers, such as the following:

> "(b) *Exemptions*. Paragraph (a) of this section shall not apply to:"[4]
>
> …(3) Victim Service Providers, defined as any nonprofit, nongovernmental organization that assists domestic violence, dating violence, sexual assault, or stalking victims, including rape crisis centers, domestic violence shelters, faith-based organizations, and other organizations, with a documented history of effective work concerning domestic violence, dating violence, sexual assault, or stalking.

---

[1] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, F.C.C. 11-41, ¶ 10 (proposed Mar. 9, 2011).
[2] *Id.* at ¶ 7.
[3] *Id.* at ¶ 23.
[4] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking Notice of Proposed Rulemaking, F.C.C. 11-41, Appendix A (proposed Mar. 9, 2011)(to be codified at 47 C.F.R. § 64).

The proposed definition comes from the Violence Against Women Act of 1994 (VAWA).[5] This definition is broad enough to encompass the range of organizations and facilities that use spoofing technology to protect victims.

Victim service providers use spoofing for legitimate purposes, and an exemption will clarify that they should not be prosecuted. For example, a victim may need to call an abuser from a program or shelter office as part of a court order to discuss custody issues, and use spoofing to ensure the abuser will pick up the call and not determine the victim's location.[6] Alternatively, domestic violence assistance programs may need to call phone lines that are not "safe"—such as lines monitored by an abusive partner—in order to check-in with a program participant, or respond to a victim call, without alerting the abuser.[7] With an exemption, these providers will feel safer in using these spoofing techniques.

The statutory history of the Act supports an exemption, under 47 U.S.C. § 227(e)(B)(ii), for uses of Caller ID spoofing that will protect victims. The 2009 Senate Commerce Committee Report on the Truth in Caller ID Act recognizes that because many phones "are set to refuse blocked or private calls," it is both "important for domestic violence shelters to transmit caller ID information so a call is completed" and potentially "necessary to alter the caller ID information to ensure the safety of domestic violence victims."[8] The 2010 House Committee on Energy and Commerce Report also acknowledges that caller ID spoofing is an important part of protecting victims of

[5] VAWA, 42 U.S.C. § 13925(a)(36) (2010).
[6] S. REP. NO. 111-96, at 2 (2009)("2009 Commerce Committee Report").
[7] *Id.*
[8] *Id.*

domestic violence stating, "domestic violence shelters sometimes use spoofing…for protective purposes…to protect [shelter residents'] identity."[9] The Commission explicitly acknowledges this "beneficial" use of spoofing in its NPRM.[10] But it does not seek to specifically exempt victim service providers from prosecution. We urge the Commission to protect "domestic violence shelters that provide false caller ID numbers to prevent call recipients from discovering the location of victims," and to prevent uncertainty and potentially costly litigation targeting victim service providers, by specifically exempting, by rule, the use of spoofing by victim service providers.[11]

II. THE COMMISSION SHOULD DEFINE "HARM" TO PROTECT VICTIMS.

The Act prohibits the use of spoofing to cause "harm" but it does not define what it means by "harm." In its rules implementing the Truth in Caller ID Act of 2009, the Commission should include a definition of the term "harm" to clarify that it covers violations of protection and restraining orders, and harms caused by stalking and harassment. Specifically, 47 C.F.R. § 64.1600 should incorporate the following definition of harm:

> *Harm.* The term "Harm" means any type of financial, physical, or emotional harm, including violating protection or restraining orders and harms caused by stalking as defined in the Violence Against Women Act of 1994, 42 U.S.C. § 13925(a) (20), (24), and harassment.

[9] H.R. REP. NO. 111-461, at 3, 6 (2010).
[10] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, F.C.C. 11-41, ¶ 7 (proposed Mar. 9, 2011)(citing 2009 Commerce Committee Report, *supra* note 5).
[11] H.R. REP. NO. 111-461, at 6-7 (2010).

Defining the Truth in Caller ID Act's language, "intent to…cause harm," to include violation of protection and restraining orders, stalking, and harassment would improve the Act's coverage of the malicious uses of caller ID spoofing and their dangerous impacts.[12] Caller ID spoofing service providers' websites are brazen about the harmful uses of their services. The Spoofem.com service provider website states, "caller id spoofing . . . [is a] term . . . commonly used to describe situations in which the motivation is considered nefarious by the speaker."[13] SpoofCard.com has a "SpoofCard Real Stories/Uses" section on its website where users of SpoofCard share their experiences with the service. The "Stories/Uses" section is filtered into four categories: pranks, personal stories, law enforcement/private investigators, and professional uses.[14] Testimonials in the personal stories category display accounts of harassment. In one, a man harassed and stalked his former wife incessantly and was only able to speak to her under the disguise of her mother's number. More importantly, the man's use of SpoofCard caused his former wife "to panic," thinking that the caller was at her mother's house:

> Totally satisfied. My ex wife would not answer the phone when she saw my name on her caller ID, so one day when after I called her all day without her answering the phone I finally decided to put her moms phone number in the caller id then she answered "hi mom" Im like this isn't your mom she said what are you doing at my moms, I told her not to worry about it, she started to panic that I was at her moms house getting some "dirt" on her for our divorce trial.[15]

---

[12] 47 U.S.C. § 227(e)(1) (2010).
[13] *What is Spoofem?*, SPOOFEM.COM (last visited Mar. 29, 2011) http://spoofem.com/about-us.
[14] *SpoofCard Real Stories/Uses*, SPOOFCARD (last visited Mar. 29, 2011), http://www.spoofcard.com/stories.
[15] *Id.*

In another the caller revels in scaring and harassing call receivers, including scaring a “kid”:

> I've fooled so many of my buddies. Calling them from their friends number and one time we said "we have him in our trunk" and the kid got so scared that he ended up telling his friend that "Mike got kidnapped" right after the call ended. Word got back around to us, it was one good prank. Most times we tell people we're "on the way" to meet them and that gets a good scare out of them. Other than that, we try not to violate victim's rights or anything.[16]

These testimonials show the types of harms that can be caused by caller ID spoofing, including harassment, intimidation, threats, and stalking. These personal stories are more than just the fun, “hysterical . . . pranks and gags” advertised by caller ID spoofing service providers.[17] These testimonials involve intimidation, stalking, and harassment.

As evidenced above, caller ID spoofing harms should encompass harassment and stalking because they cause substantial emotional distress and cause victims to fear for their safety or the safety of others.[18] Violations of protection and restraining orders should also be considered caller ID spoofing harms because protection and restraining order are meant to protect victims from harassment, and unwanted contact, and communication with abusers. VAWA defines “protection order” or “restraining order” as:

> (A) any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment against, sexual violence or contact or communication with or physical proximity to, another person, including any temporary or final orders issued by civil or criminal courts whether obtained by filing an independent action or as a pendent lite order in another proceeding so long

---

[16] *Id.*
[17] *Who’s Using Bluff My Call*, BLUFFMYCALL.COM (last visited Mar. 30, 2011), http://bluffmycall.com/testimonials.
[18] VAWA, 42 U.S.C. § 13925(a)(24) (2010).

as any civil order was issued in response to a complaint, petition or motion filed by or on behalf of a person seeking protection; and

(B) any support, child custody or visitation provisions, orders, remedies, or relief issued as part of a protection order, restraining order, or stay away injunction pursuant to State, tribal, territorial, or local law authorizing the issuance of protection orders, restraining orders, or injunctions for the protection of victims of domestic violence, dating violence, sexual assault, or stalking.[19]

Therefore, to extensively address harms such as harassment and stalking, it is imperative to include violations of court orders designed to prevent those harms.

NNEDV has found that misuse of technology, as illustrated in the examples above, increases abusers' opportunities to "harass, terrify, intimidate, coerce, and monitor former and current intimate partners."[20] Abusers misuse technology to "stalk [their victims] before, during, and after perpetrating sexual violence."[21] The impacts of stalking and harassment—which can result from caller ID spoofing misuse as shown in SpoofCard's "Stories"—are alarming. In June 2009, the Department of Justice reported "3.4 million people over the age of 18 are stalked each year in the United States," with 25% of victims reporting "being stalked through the use of some form of technology."[22] Almost half of stalking victims endure "at least one unwanted contact per week."[23] The Journal of Interpersonal Violence reports "the prevalence of anxiety, insomnia, social dysfunction, and severe depression is much higher among stalking victims than the

---

[19] VAWA, 42 U.S.C. § 13925(a)(20) (2010).
[20] National Network to End Domestic Violence, Safety Net Project, *High-Tech Stalking, 2009*, http://www.nnedv.org/docs/SafetyNet/NNEDV_HighTechStalking_TipsForAgencyPartners.pdf.
[21] *Id.*
[22] BUREAU OF JUSTICE STATISTICS, U.S. DEPARTMENT OF JUSTICE, NCJ 224527, NATIONAL CRIME VICTIMIZATION SURVEY: STALKING VICTIMIZATION IN THE UNITED STATES, 1 (2009).
[23] *Id.*

general population."[24] A clear definition of "harm" is necessary to address the gravely destructive impacts of caller ID spoofing.

III. THE COMMISSION SHOULD REQUIRE THIRD-PARTY CALLER ID SPOOFING SERVICES TO GIVE PROMINENT NOTICE THAT USE OF THEIR SERVICES IN VIOLATION OF THE TRUTH IN CALLER ID ACT IS UNLAWFUL.

Third-party spoofing services, such as SpoofCard, fail to adequately inform consumers of unlawful uses of caller ID spoofing, and may even promote such uses. The Commission inquires about obligations to be imposed on providers of spoofing services.[25] The Commission should require that Spoofing services providers give their users notice that spoofing calls in violation of the Truth in Caller ID Act subjects them to criminal and civil liability, and is an impermissible use of caller ID spoofing.

A. Existing Notices of Truth in Caller ID Act Violations are Inadequate and Contradictory.

Although many caller ID spoofing service websites contain small print legal disclaimers addressing unlawful or impermissible use of their services, **[26]** the following screenshot from SpoofCard is indicative of the attitude service providers have toward caller ID spoofing regulation.

---

[24] Ella Arensman, Eric Blaauw, Adriënne Freeve, Lorraine Sheridan & Frans Winkel, *The Toll of Stalking: The Relationship Between Features of Stalking and Psychopathology of Victims*, 17 J. INTERPERSONAL VIOLENCE, no. 1, 2002 at 50, 57.
[25] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, F.C.C. 11-41, ¶ 21 (proposed Mar. 9, 2011)
[26] *Terms of Service*, BLUFFMYCALL.COM (last visited Apr. 7, 2011), , http://bluffmycall.com/terms.

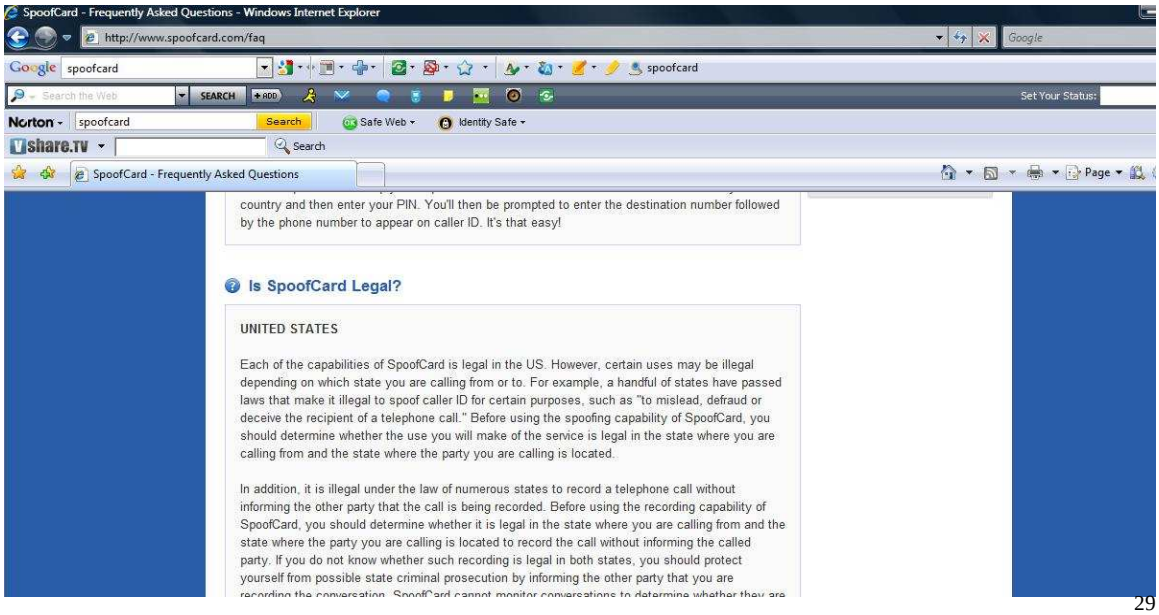
[27]

SpoofCard mocks Truth in Caller ID Act legislation, and its legal disclaimer—and the disclaimers of similar services—does not provide sufficient information to customers about unlawful caller ID spoofing.

Currently, caller ID spoofing services market caller ID spoofing as fully legal.[28] The following are examples of the small print legal disclaimers from caller ID spoofing service provider websites.

[27] *SpoofCard's Stance On The Truth in Caller ID Act*, SPOOFCARD (Apr. 19, 2010), http://www.spoofcard.com/blog/2010/04/19/spoofcards-stance-on-the-truth-in-caller-id-act.

[28] PHONEGANGSTER.COM (last visited March 31, 2011), http://www.phonegangster.com.



29

SpoofCard

To find information regarding permissible and impermissible uses of SpoofCard, users have to select the "Frequently Asked Questions" area of the SpoofCard website, because the website does not have a "Terms of Service" section where users can find that information.[30] The fact that permissible and impermissible uses are not prominently displayed makes it unlikely that users of spoofing services will access, and use, such information when spoofing. In the "Frequently Asked Questions" area of its website, SpoofCard answers "Is SpoofCard Legal?":

> Each of the capabilities of SpoofCard is legal in the US. However, certain uses may be illegal depending on which state you are calling from or to. For example, a handful of states have passed laws that make it illegal to spoof caller ID for certain purposes, such as "to mislead, defraud or deceive the recipient of a telephone call." Before using the spoofing capability of SpoofCard, you should determine whether the use you will

[29] *Frequently Asked Questions*, SPOOFCARD(last visited Apr. 5, 2011), http://www.spoofcard.com/faq.
[30] SPOOFCARD (last visited April 11, 2011), http://www.spoofcard.com.

> make of the service is legal in the state where you are calling from and the state where the party you are calling is located.[31]

SpoofCard's half-hearted legal explanation does not give adequate notice of Truth in Caller ID Act liability. Their answer does not adequately inform users of the legal risks one faces when impermissibly using caller ID spoofing services. SpoofCard says that some uses "may be illegal depending upon which state [one is] calling from or to," and references without citation some nebulous state laws.[32] However, SpoofCard is aware that impermissible uses of caller ID spoofing are no longer regulated solely by state law, but to the contrary there is a federal law, applicable in all states, making it illegal to use SpoofCard services to "defraud, cause harm or wrongfully obtain anything of value."[33] Additionally, SpoofCard's explanation of the legal uses of its service only addresses the caller and the receiver, but not the third-party whose number the caller is impersonating.

Elsewhere on SpoofCard's website, specifically on the SpoofCard Blog, users are told "Caller ID Spoofing is NOT illegal" and SpoofCard even quotes statutory language from the Truth in Caller ID Act to tell users "as long as you are using our service in a lawful manner and not with the intent to 'defraud, cause harm or wrongfully obtain anything of value', you can continue to use SpoofCard just as you have prior to [the Truth in Caller ID Act] being enacted."[34] However, as displayed above in the "Stories" section of SpoofCard.com, SpoofCard users have used SpoofCard to cause harm through

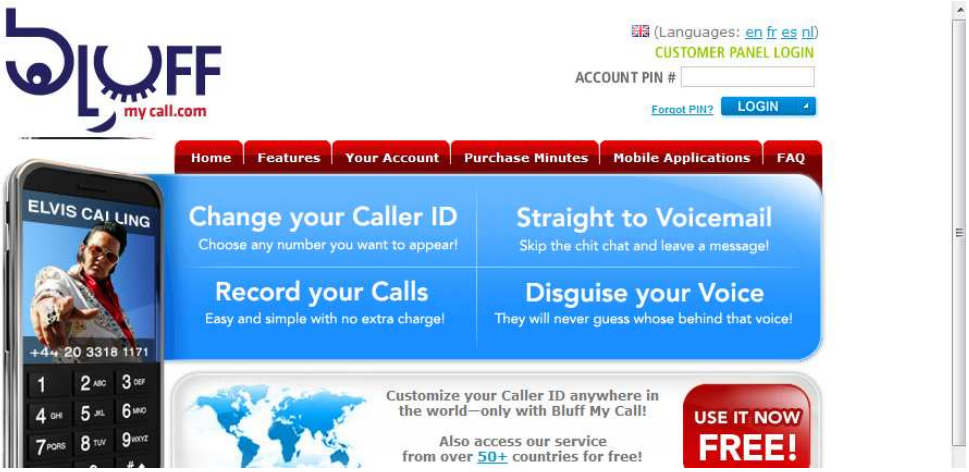
---

[31] *Frequently Asked Questions*, SPOOFCARD (last visited Apr. 5, 2011), http://www.spoofcard.com/faq.
[32] *Id.*
[33] *An Update On S. 30: The Truth in Caller ID Act of 2009*, SPOOFCARD (Jan. 6, 2011), http://www.spoofcard.com/blog/2011/01/06/an-update-on-s-30-the-truth-in-caller-id-act-of-2009.
[34] *Id.*

intimidation, harassment and stalking. Thus, SpoofCard's disclaimer does not adequately apprise SpoofCard users of illegal caller ID spoofing uses.

We urge the FCC to mandate that SpoofCard and comparable services give unequivocal notice that user of their services in violation of the Truth in Caller ID Act is unlawful. Such notice would resolve the contradictions caused by simultaneous small print disclaimers of illegal caller ID spoofing and the promotion of illegal caller ID spoofing.

BluffMyCall.Com



[35]

In its Terms of Service "Acceptable Use of Service" clause, caller ID spoofing company BluffMyCall.com informs users that they

> shall not transmit any unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, sexually explicit, profane, hateful, racially, ethnically, or otherwise objectionable material of any kind, including but not limited to any material that encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable local, state, national, or international law

[35] BLUFFMYCALL.COM (last visited Apr. 7, 2011), http://bluffmycall.com.

and that violation of any laws, or violation of the Terms of Service, may lead to termination the user account with BluffMyCall.com.[36] However, one of the promotions for their service emphasizes users' ability to do "hysterical stuff, like the pranks and gags."[37] By promoting "pranks and gags" as an acceptable use of the service, BluffMyCall.com does not sufficiently place users on notice that some "pranks and gags" are illegal, and is therefore encouraging potentially illegal behavior.

Phone Gangster

[38]

Phone Gangster promotes its services as "fun" and "legal," however there is no place on its website where users can learn what are legal and illegal forms of caller ID spoofing. [39]

---

[36] *Terms of Service*, BLUFFMYCALL.COM (last visited Apr. 7, 2011), http://bluffmycall.com/terms.
[37] *Who's Using Bluff My Call*, BLUFFMYCALL.COM (last visited Mar. 30, 2011), http://bluffmycall.com/testimonials.
[38] PHONEGANGSTER.COM (last visited Mar. 31, 2011), http://www.phonegangster.com.

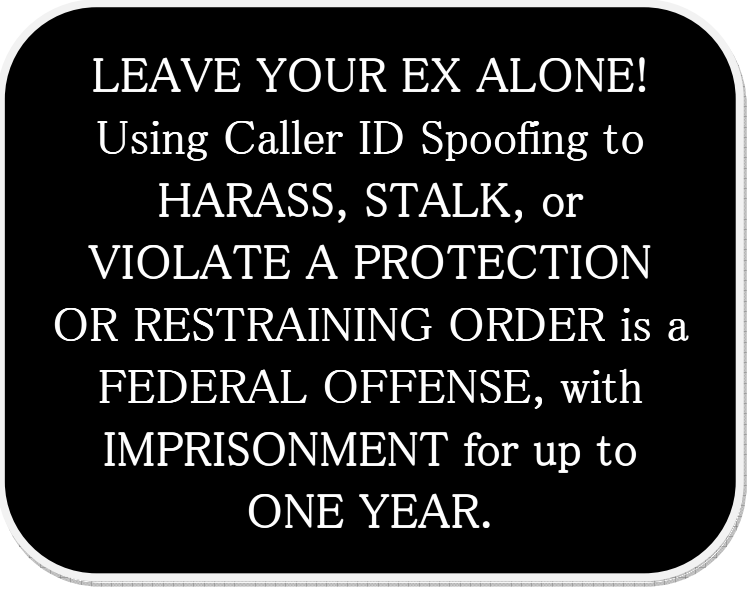
B. Requiring Third-Party Prominent Notice Of The Legal Ramifications Of Caller ID Spoofing Misuse Should Discourage Impermissible Caller ID Spoofing.

Adequate of caller ID spoofing in violation of the Truth in Caller ID Act should provide clear guidelines on prohibited behavior. As mentioned above, the small print disclaimers currently used by caller ID spoofing services are wholly inadequate to inform users of the relevant law or the legal risks one faces when impermissibly using caller ID spoofing services. Furthermore, the website "disclaimers" of unlawful caller ID spoofing contradict the website promotions of unlawful caller ID spoofing. In the future, the Commission should require providers of these services to have multiple, easily accessible notices on their websites which warn that violations of the Truth in Caller ID Act will subject violators to criminal and civil liability, as well as subject them to termination of their account with the company. The Commission should also require audible notice before each call is made. The following are examples of notices that NNEDV recommends:

[39] *Id.*

CAUTION: THINK BEFORE YOU SPOOF! The misuse of this service to DEFRAUD, HARASS, STALK, VIOLATE A RESTRAINING OR PROTECTION ORDER, or WRONGFULLY OBTAIN ANYTHING OF VALUE is a FEDERAL CRIME and will subject you to IMPRISONMENT for up to ONE YEAR AND CRIMINAL FINES up to $10,000 for EACH VIOLATION AND CIVIL PENALTIES up to $1,000,000. Your account with our company will also be terminated if you misuse our services in the ways mentioned above.

WARNING: The misuse of this service to HARASS is a FEDERAL CRIME and will subject you to IMPRISONMENT for up to ONE YEAR AND CRIMINAL FINES up to $10,000 for EACH VIOLATION AND CIVIL PENALTIES up to $1,000,000. Your account with our company will also be terminated if you misuse our services in the ways mentioned above.



The Commission should require text of warnings such as these—not just hyperlinks to warnings on another webpage— to be placed on every individual webpage of service providers' websites. Moreover, in order to make such notice effective and

legible, the text of the warnings should be as prominently displayed as other marketing on the website. Finally, an audible recording of a warning should play over the phone before a caller is able to place a spoofed call. Such prominent notice of the legal ramifications of misuse of caller ID spoofing should effectively dissuade illegal caller ID spoofing.

IV. THE COMMISSION SHOULD REQUIRE CALLER ID UNMASKING SERVICES TO NOTIFY CALLERS, AND PROVIDE THEM WITH THE ABILITY TO "OPT-IN," WHEN THEIR PRIVACY INDICATOR IS BEING OVERRIDDEN.

The Commission seeks comments on the topic of unmasking, which overrides a calling party's privacy choice.[40] We request that the Commission impose obligations on unmasking service providers to notify callers when their blocked caller ID will be unmasked and to require affirmative opt-in consent before they are unmasked. Companies that offer services to unmask blocked caller ID are potentially endangering victims by allowing their abusers to see their hidden phone numbers. If the Commission fails to regulate caller ID unmasking services there is a strong potential for harm. Indeed, unmasked caller ID could have fatal consequences for victims of ongoing domestic violence.[41]

One example of a provider of caller ID unmasking is TrapCall, which the Commission identified as a product that is "effectively stripping out the [caller ID]

---

[40] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, F.C.C. 11-41, ¶ 27 (proposed Mar. 9, 2011).

[41] *See* Emily Friedman, *TrapCall Unblocks Caller-ID, Exposes Number*, ABC NEWS (Feb. 18, 2009), http://abcnews.go.com/Technology/AheadoftheCurve/story?id=6899472&page=3 ("it could result in more cases like the 1995 murder of 21-year-old Kerisha Harps, who was killed by her ex-boyfriend when he saw the number where she was calling from on a Caller ID display").

privacy indicator chosen by the calling party."[42] TrapCall utilizes conditional call forwarding to implement its service—and bounces the forwarded call back to the subscriber's phone—which entails that the calling party will not know her call is forwarded to a third party for unmasking because the line is continually ringing.[43] Some unblocking services (and earlier versions of TrapCall) exploit a loophole in the Commission's rules by forwarding incoming calls to a toll free number to access blocked caller ID,[44] however routing through an interconnected VoIP (Voice over Internet Protocol) service appears to be the current method of choice.[45] Both of these methods ensure that a caller with legally blocked caller ID will be unaware that her information has been disclosed to the person called, threatening both her privacy and safety, because they involve an unknown third party.

The Truth in Caller ID Act of 2009 was designed with preservation of caller ID blocking in mind.[46] Congress wanted to ensure it would not "prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information" through the Act.[47] "By FCC regulation, consumers…have the right to conceal their [caller ID]," and this rulemaking is an appropriate venue to protect

---

[42] *Id.*
[43] *See FAQ*, TRAPCALL (last visited Mar. 30, 2011), http://www.trapcall.com/faq.
[44] WaybackMachine, *TrapCall-Learn More!*, INTERNET ARCHIVE (Apr. 25, 2009), http://replay.waybackmachine.org/20090425200706/http://www.trapcall.com/learnmore.
[45] "Our number that you'll want to forward your calls to is 1-206-299-2100." *FAQ*, TRAPCALL (last visited Mar. 30, 2011), http://www.trapcall.com/faq.
[46] 47 U.S.C. § 227(e)(2) (2010); *see* S. REP. NO. 111-96, at 2 (2009); H.R. REP. NO. 111-461, at 3 (2010).
[47] 47 U.S.C. § 227(e)(2) (2010).

and reinvigorate that right.[48] Without a rule on this issue, companies like TrapCall will be able to terminate consumers' right to caller ID anonymity without warning or recourse.

A. Congress and the Commission Have Long Recognized an Interest in Protecting a Calling Party's Privacy Indicator.

Forwarding calls through a service such as TrapCall, which does not notify calling parties it is in operation, works against the intention of the rules adopted by the FCC in 1995 implementing caller ID privacy.[49] These rules require the privacy indicator be respected "unless the call is made to a called party that subscribes to an [automatic number identification] or charge number based service and the call is paid for by the called party."[50] When these rules were promulgated sixteen years ago, the Commission did not conceive of a consumer-friendly, easily used, and readily available phone line trap service.[51] The rules are written so that a caller will have some warning or notice that her caller ID might be unmasked or reused in certain situations—such as calling a toll-free number or charge service—and that otherwise it will be unmasked only in conjunction with legitimate business or government action. Specifically, the Commission intended that a consumer be on notice that her caller ID will be revealed if she calls a business or organization with an 800- or 900- number that reverses the call charges, and

[48] S. REP. NO. 111-96, at 2 (2009).
[49] 47 C.F.R. § 64.1601 (2010).
[50] *Id.* at § 64.1601(b).
[51] *See, e.g.*, *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, 11707-08 (1995).

required 800 numbers to seek consent for reuse of automatic number identification data.[52] Combined with rules exempting private branch exchange (PBX) systems, this is the only business exception to the caller ID unblocking rule.[53] Further, the rules do not provide an exemption for private phone trapping, but only "legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency."[54]

We ask the Commission to preserve citizens' legitimate expectation of caller ID privacy when calling a private number with an active privacy indicator. Conditional call forwarding through third-party unmasking services—that in some cases may also be recording the conversation—ensures the calling party will have no notion her choice to use caller ID blocking is being circumscribed and rendered moot.[55]

It is currently within the technical ability of unmasking service providers, such as TrapCall, to provide notice and opt-in choice to callers that their caller ID privacy indicator will be overridden. For example, in response to state laws regulating call recording, TrapCall provides its Call Recording subscribers with the ability to play a warning to parties on the call.

> TrapCall has set its services up so that when you activate the automatic call recording feature, each caller hears a message before the call is answered informing them that the call will be recorded and telling them to hang up if they do not want the call to be recorded. You have the ability to override the default and choose not to have the warning message played to callers. However, we recommend strongly that you not choose this option,

---

[52] *Rules and Polices 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, ¶¶ 57-58 (1994).
[53] *See* 47 C.F.R. §§ 64.1601-1604 (2010).
[54] *Id*. at § 64.1601(d)(4)(iii).
[55] *Sign Up – TrapCall*, TRAPCALL (last visited Mar. 30, 2011), http://www.trapcall.com/signup.

> as failure to provide such notice may leave you open to criminal liability in a dozen or more states.[56]

This shows that parties can easily be provided with a choice when faced with the possibility of caller ID unmasking, and that services should be regulated to ensure implementation. The Commission should seek to have such a solution in operation industry-wide to maintain the integrity of blocked-ID call privacy.

B. Callers Should Be Provided Choice, in the Form of an Opt-In, When a Third Party Will Unmask Their Caller ID.

We ask the Commission to preserve consumers' expectation of the efficacy of caller ID blocking privacy protection. The Commission can prescribe a rule echoing the language of the Truth in Caller ID Act, requiring that third-party caller ID unmasking services provide callers with notice that the service is in place and give them the ability to opt-in to providing their caller ID to the call recipient. This would allow use of unmasking services to continue while preserving the intent of both Congress and the Commission to protect the privacy preference indicator for caller ID blocking. We ask the Commission to adopt language under 47 C.F.R. § 64.1604 stating:

> (d) Services that 'unmask' or reveal caller identification information of calls being forwarded to their service, for the purpose of providing such information to the intended call recipient ("unmasking service"), are required to provide notice, and obtain affirmative opt-in consent from the calling party, before overriding the calling party's privacy choice indicator and providing the calling party's caller identification information to the intended call recipient.

[56] *FAQ*, TRAPCALL (last visited Mar. 30, 2011), http://www.trapcall.com/faq.

V. THE COMMISSION SHOULD INCLUDE AN ANALYSIS OF THE THREATS FOR SMS AND LOCATION SPOOFING IN ITS REPORT TO CONGRESS.

The Commission inquires about successor technologies and other issues to include in its report to Congress.[57] The Commission should report on SMS and location spoofing. Both offer the same potential as caller ID spoofing – the abilities of innocent parties to protect themselves and the ability of nefarious parties to cause harm.

The Commission's report to Congress should include SMS spoofing as another potential source of harm. SMS spoofing "allows one to change the name or number text messages come from."[58] Spoofing provider Spoofcard recently launched its service for SMS spoofing.[59] Described as their "most frequently requested feature over the years" it was released "just in time for April Fools' day."[60] SpoofCard further claims that it is the "ONLY company in the world that you will find capable of doing true text message spoofing to US phone numbers."[61] However, other providers promise SMS spoofing capability, such as FakeMyText[62], Spooftel,[63] and Fakemsg.[64] SMS messages can carry the same potential for harm as voice calls.

Further successor technologies to report on are location-based services. These services allow users to send messages about their current location. For example,

---

[57] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, F.C.C. 11-41, ¶ 35 (proposed Mar. 9, 2011).
[58] SMS SPOOFING, (last visited Apr. 18, 2011), http://www.smsspoofing.com/.
[59] *SMS Spoofing Launches Just In Time For April Fools' Day!*, SPOOFCARD (Mar. 31, 2011), http://www.spoofcard.com/blog/2011/03/31/sms-spoofing-launches-just-in-time-for-april-fools-day.
[60] *Id.*
[61] *Id.*
[62] FAKEMYTEXT (last visited Apr. 12, 2011), http://www.fakemytext.com.
[63] *Frequently Asked Questions*, SPOOFTEL (last visited Apr. 12, 2011), http://www.spooftel.com/caller+id+spoofing+faq.html.
[64] *Tell Me More*, FAKEMSG (last visited Apr. 12, 2011), http://www.fakemsg.com/faq.php.

Facebook places allows users to share their location, connect with nearby friends, search for location based promotions, and "check in" other users to their current location.[65] These user actions cause messages to be sent out to a user's connections on Facebook updating them that the user is at the location.[66] Other location based services work similarly.

Several sources have pointed out the possibility of location spoofing.[67] A service may allow a user to set a location that they are not presently at as a feature. Or the spoofing might be accomplished via a third party or other technological technique in violation of the location service's terms of use.

Like caller ID spoofing, location spoofing can be used for beneficial purposes, such as allowing a user to set their location at a public library while they visit a victim service provider. This provision of a location "alibi" might be an important safety consideration for someone in an abusive situation whose abuser has forced them to share their location. On the other hand, location spoofing can be used to cause harassment and other harms in several ways. First, a location service can send a message that someone is at a particular location, thus fooling the recipient. Second, some services may allow an individual to view who is at their location, thus allowing a spoofer to see who else is at that location. Third, some services allow an individual to check-in others at the

---

[65] *Places*, FACEBOOK (last visited Apr. 12, 2011), https://www.facebook.com/places.
[66] *Id.*
[67] *Location Spoofing Possible with Wi-Fi Devices: Positioning System Used by Iphone/Ipod Breached*, SCIENCEDAILY (Apr. 16, 2008), http://www.sciencedaily.com/releases/2008/04/080414145659.htm; Greg Norcie, *How To Spoof Facebook Places Location Data in Firefox* (Aug. 20, 2010), http://blog.norcie.com/2010/08/how-to-spoof-facebook-places-location.html; Zack Whittaker, *How to spoof your geolocation on Facebook Places or Twitter*, ZDNET (Nov. 16, 2010), http://www.zdnet.com/blog/igeneration/how-to-spoof-your-geolocation-on-facebook-places-or-twitter/6764.

individual's location, thus allowing a spoofer to spoof check-ins at the location. These spoofed check-ins could cause location messages to be sent to the victim's friends.

CONCLUSION

The Commission should exempt victim service providers from coverage of the act. The Commission should clarify that prohibited harms include stalking, harassment, and the violation of protective orders. The Commission should require prominent notice of criminal penalties from spoofing providers. Unmasking providers should provide a notice and require affirmative opt-in consent before removing caller's privacy indicators. Finally, the Commission should report to Congress on SMS and location spoofing.

Respectfully submitted,

Cindy Southworth
Vice President of Development & Innovation
2001 S St NW, Suite 400
Washington, DC 20009
phone: 202-543-5566
fax: 202-543-5626

Guilherme Roschke, Esq.
Angela Campbell, Esq.
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9535

Counsel for National Network to End Domestic Violence

Khaliah Barnes
Samuel Philipson

Law Students
Georgetown Law

April 18, 2011