S. HRG. 110–1139

CALLER ID SPOOFING

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 21, 2007

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

74–894 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, *Vice Chairman*
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	TRENT LOTT, Mississippi
BARBARA BOXER, California	KAY BAILEY HUTCHISON, Texas
BILL NELSON, Florida	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	GORDON H. SMITH, Oregon
FRANK R. LAUTENBERG, New Jersey	JOHN ENSIGN, Nevada
MARK PRYOR, Arkansas	JOHN E. SUNUNU, New Hampshire
THOMAS R. CARPER, Delaware	JIM DEMINT, South Carolina
CLAIRE MCCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	JOHN THUNE, South Dakota

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
KENNETH R. NAHIGIAN, *Republican Deputy Staff Director and Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

CALLER ID SPOOFING

THURSDAY, JUNE 21, 2007

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 11:03 a.m., in room SR–253, Russell Senate Office Building, Hon. Bill Nelson, presiding.

OPENING STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator NELSON. Good morning. Over the past few years, consumers have been hit with a number of new scams that seek to use our Nation's telecommunications network for fraudulent purposes, from pretexting to spyware. Fraudsters are always looking for new ways to invade our privacy and personal and financial information and one of the newest scams is called Caller ID Spoofing.

It's a technique that allows a telephone caller to alter the telephone number and other information that appears on the recipient's Caller ID system. It's an easy scam to pull. All an individual needs to do is go to one of a number of Internet sites with names like *Tricktell.com* and *SpoofTell.com*, to gain access to spoofing services and on these sites, an identify thief can pay money to order a spoofed telephone, tell the website what telephone number they wish to reach and then place a spoofed telephone call through a toll-free line. A number of recent news stories have highlighted the serious harm that is caused by this practice.

One recent example—fraudsters used Caller ID spoofing to pose as court officers calling to say that the individual had missed jury duty. The caller then says that a warrant will be issued for their arrest unless they pay a fine with a credit or bank card during the call and you know what the result is going to be.

In another case, identity thieves and criminals have used Caller ID spoofing to hack into a bank account and into voicemail accounts to steal sensitive personal information.

Now while these examples are serious enough, just think what could happen if a stalker used Caller ID spoofing to trick someone into answering their phone and providing information on where they are and the results could be tragic. So it's time to put an end to Caller ID spoofing.

The bipartisan Truth in Caller ID Act of 2007 will plug the hole in the current law and make it clear that spoofing is a scam and is not legal. So it is my privilege to chair this hearing on behalf

of Senator Inouye and the Vice Chairman of the Committee, I would turn to him, Senator Stevens.

STATEMENT OF HON. TED STEVENS,
U.S. SENATOR FROM ALASKA

Senator STEVENS. Thank you very much, Senator. I'm grateful to Senator Inouye for calling this hearing. These ID services provide us all with information that we need. Really, I'm delighted to have the information. When I see who is calling me, I can tell whether to pick it up right away or ask my staff to deal with it if it is something that I don't have the time for.

This idea that some people can alter that ID information bothers me considerably because it means that a loss of privacy means identity theft possibilities and really as Senator Nelson has mentioned, can compromise personal safety. We need to understand those concerns and to try to make a record and that's what we're going to do today with your help so that others will review what this panel gives us to determine what holes are in our laws and if they can be filled to address and prevent this spoofing practice.

I'm particularly worried about the fraudulent aspects that Senator Nelson has mentioned, particularly where it could lead to obtaining money under totally false pretenses. It ought to be against the law already but I want to find out if there is any way and anyone in law enforcement working to deal with that directly at this time. Senator Nelson, Senator Snowe and Senator McCaskill have introduced this bill. It's going to come before the Committee next week and this will be the only hearing, the only opportunity we have to get a record for other members to learn about this. So I'm particularly concerned about the law enforcement actions that have been taken. I congratulate the sponsors but will it provide the tools that law enforcement needs to really improve enforcement activities and will it provide the information that is necessary?

I'd like to see something developed and invented so that if I see something on my Caller ID that I want to preserve then I could transfer it. We lose that immediately—once we hang up, we've lost that ID. What the telephone records might show would be one thing but what has shown on ID is another thing, is my understanding. Though somehow or another, we've got to be able to find a way to preserve that information to show the fraudulent activities involved. And we get a great many calls from around the country and when we get a Caller ID that indicates to us it's a governor or it's someone from major organization and we're working on that legislation, we ought to be able to rely on that ID.

This fraudulent ID concept goes to really, I think contact violating the Constitutional concept that people have the right to contact Congress to redress wrongs, but if they are contacting us under false pretences, we've got to have a way to know it. So I think this is a very important piece of legislation. I do hope the record will help us convince the other members of the Committee of that fact.

I look forward to the hearing. Unfortunately, I have to go somewhere at half past, so I'll wrap up.

Senator NELSON. Well, Senator Stevens, thank you for your encouraging and supportive comments. And here's another example.

A couple of years ago, a sharp-shooting SWAT team shut down a neighborhood in New Brunswick, New Jersey, after they received what they thought was a distress call coming from an apartment in the neighborhood and it turned out it was a spoof call and it put a lot of lives at risk, time after time.

Well, we've got a distinguished panel. Ms. Kris Monteith, Chief of the Enforcement Bureau of the FCC, Mr. Jerry Cerasale, Senior Vice President of Government Affairs of the Direct Marketing Association, Ms. Allison Knight, Staff Counsel and Director of Privacy and Human Rights Project, Electronic Privacy Information Center and Mr. Ron Jones, Director of the Tennessee Regulatory Authority and Chairman of the Consumer Affairs Committee of the National Association of Regulatory Utility Commissioners. So welcome, all.

Your written statements are entered into the record and because of the constraints of time, I would appreciate it if you could talk directly to us. We'll go right in the order in which I introduced you, without you reading your testimony to us because we're going to have it as part of the record, if you would give us your thoughts. So let's start with you, Ms. Monteith.

STATEMENT OF KRIS ANNE MONTEITH, CHIEF, ENFORCEMENT BUREAU, FCC

Ms. MONTEITH. Good morning. Thank you very much, Vice Chairman Stevens, Senator Nelson and members of the Committee. Thank you for the opportunity to speak with you today about the problem of caller identification spoofing. As you've stated, Caller ID services lets customers identify who's calling them before they pick up the phone, such as by a telephone number, a name or business number displayed on the customer's equipment. Caller ID spoofing refers to the practice in which the Caller ID information is manipulated in a manner that misleads the call recipient about the identity of the caller.

The Commission is deeply concerned about reports that Caller ID information is being manipulated for fraudulent or deceptive purposes and the impact of those practices on the public trust and confidence in the telecommunications industry.

We are particularly concerned about how this practice may affect consumers as well as public safety and law enforcement communities. I think you're aware of some of the technical means by which caller identification travels with the phone call so I won't go into detail and I think that information is in my written testimony.

The Commission also has addressed caller identification on the public switched telephone network in rules that were adopted in 1995 and generally, those rules require all carriers using Signaling System 7—SS7—to transmit the calling party number associated with an interstate call to interconnecting carriers. This same Commission rule also requires telemarketers to transmit accurate Caller ID information.

With the development of the Internet and IP technologies, Caller ID spoofing has apparently been made easier—even easier than it used to be. Now entities using IP technology can generate false calling information and pass it to the PSTN via SS7.

The Commission's Enforcement Bureau has been investigating this practice since it came to our attention in the summer of 2005,

having come to our attention in the context of junk fax spoofing. To date, we have initiated investigations on 13 companies engaged in the marketing and selling of Caller ID spoofing services to customers. One investigation has resulted in a citation against a telemarketer called Intelligent Alternatives for rule violations including violations of the Caller ID rules under Section 64.1601 of our rules.

We've sent formal Letters of Inquiry to these entities and, at the same time, served subpoenas on them to compel them to respond to our inquiries. In some cases, we followed up with subsequent Letters of Inquiry to uncover additional evidence of possible violations.

Importantly, our investigations have revealed that the companies that are engaged in these practices are of varying degrees of sophistication that employ disparate methods and technologies to provide service to different types of customers. Some of the companies, for example, claim that they are involved in legitimate activities, providing spoofing services only to customers such as law enforcement officials, private investigators, or to others that are engaged in the furtherance of debt collection or other similar types of activities.

The companies allow customers to customize, so to speak, the services that they select. For example, in some cases, the spoofing companies claim that they do not allow the customer to decide the particular false number to be displayed on the called parties' ID while others do provide that functionality. This functionality is very important because it implicates whether or not a spoofer would permit the customer to use 911 as a spoofed number or whether the customer could, for example, choose another telephone number that might be a government number—and as you suggest, Senator Nelson—or the number of other emergency services providers.

The Enforcement Bureau is continuing to gather and analyze information about the companies' practices, their network, businesses, and customers, and other relevant matters that will assist us in fully understanding the issues and whether violations of the Communications Act have, in fact, occurred.

In addition to our enforcement efforts, the Commission has taken steps to prevent those engaged in Caller ID spoofing for deceptive reason from successfully accessing the personal information of telecommunications customers. In a recent order tightening the Commission's Customer Proprietary Network Information rules, we determined that a carrier providing call history information over the phone to a customer must first call that customer back at the telephone number of record to ensure that the individual calling is, in fact, the customer rather than relying on the Caller ID as an authentication method, thereby eliminating one of the major tools of pretexters.

As we've testified previously, the Commission may not have sufficient authority to fully address this issue of spoofing. Some of the entities under investigation, do not appear to be directly regulated by the Commission and, in fact, they've made this assertion in response to our investigations. Thus, legislation that clarifies the Commission's authority in this area would be helpful.

In conclusion, just to reiterate that the intentional manipulation of Caller ID information is an issue of importance to the Commission, particularly where it is used for fraudulent or deceptive reasons. We look forward to working with members of the Committee and other Members of Congress to ensure that the public maintains its confidence in the telecommunications industry. Thank you.

[The prepared statement of Ms. Monteith follows:]

PREPARED STATEMENT OF KRIS ANNE MONTEITH, CHIEF, ENFORCEMENT BUREAU, FCC

Good morning Chairman Inouye, Vice Chairman Stevens and members of the Committee. Thank you for the opportunity to speak about the problem of caller identification (Caller ID) spoofing.

As you know, Caller ID services let customers identify who is calling them before they answer a call by displaying the caller's telephone number or other information—such as a name or business name—on the customer's equipment before the customer picks up the phone. "Caller ID spoofing" refers to a practice in which the Caller ID information transmitted with a telephone call is manipulated in a manner that misleads the call recipient about the identity of the caller. The use of Internet technology to make phone calls has apparently made Caller ID spoofing even easier. The Commission is deeply concerned about reports that Caller ID information is being manipulated for fraudulent or other deceptive purposes and the impact of those practices on the public trust and confidence in the telecommunications industry. We are particularly concerned about how this practice may affect consumers as well as public safety and law enforcement communities.

In my testimony, I will first provide a brief technical background on Caller ID spoofing. Then, I will describe the Commission's rules addressing Caller ID services and the steps the Commission is taking to make sure that providers are fully meeting their obligations under the Communications Act and the Commission's rules and orders.

As a technical matter, Caller ID spoofing happens by manipulating the data elements that travel with a phone call. Phone calls on the public switched telephone network, or PSTN, are routed to their destinations by means of a specialized protocol called the Signaling System 7, or SS7. SS7 conveys information associated with a call such as the telephone number of the caller. The SS7 information for a call is provided by the carrier that the caller uses to place the call. Caller ID then displays that caller's number to the called party. Caller ID spoofing is accomplished by manipulating the SS7 information associated with the call.

The Commission addressed Caller ID on the PSTN in 1995 with rule 64.1601, which generally requires all carriers using SS7 to transmit the calling party number associated with an interstate call to interconnecting carriers. The same Commission rule also requires telemarketers to transmit accurate Caller ID information.

The development of Internet and IP technologies has made Caller ID spoofing easier than it used to be. Now, entities using IP technology can generate false calling party information and pass it into the PSTN via SS7. Caller ID spoofing can potentially threaten our public safety. For example, spoofers can fabricate emergency calls and cause local law enforcement and public safety agencies to deploy their resources needlessly. Caller ID spoofing can potentially threaten consumers. For example, spoofing can be used by the unscrupulous to defraud consumers by making calls appear as if they are from legitimate businesses or government offices.

The Commission's Enforcement Bureau (Bureau) has been investigating the issue of Caller ID spoofing since the summer of 2005 when information regarding junk fax spoofing came to our attention. To date, the Bureau has initiated investigations of thirteen companies engaged in the marketing and selling of Caller ID spoofing services to customers. One investigation resulted in a citation against a telemarketer, Intelligent Alternatives, for rule violations, including violations of the Caller ID rules under section 64.1601. We have sent formal Letters of Inquiry and, at the same time, served subpoenas to compel responses to our inquiries. In some cases, we have issued subsequent Letters of Inquiry to uncover additional evidence of possible violations of the Communications Act.

Our investigations have revealed that the companies engaged in this practice are of varying degrees of sophistication that employ disparate methods and technologies to provide service to different types of customers. Some of the companies, for example, claim they are providing spoofing services only to customers such as law en-

forcement officials or private investigators, or to others engaged in the furtherance of debt collection and other similar objectives. The companies also allow customers varying amounts of flexibility over the spoofing: some companies claim they do not allow customers the ability to customize the false number to be displayed on the called party's Caller ID while others do provide that functionality. This last characteristic is particularly important when determining whether spoofers permit their customers to use "9-1-1" as a spoofed number or whether the customers can spoof the numbers of first responders and other emergency services providers. We are continuing to seek relevant information to assist us in fully understanding these issues and whether violations of the Communications Act or our rules have occurred.

We also have held meetings with numerous industry representatives, including wireline, wireless, and Voice over Internet Protocol (VoIP)-based companies, to determine the impact of Caller ID spoofing on their consumers and networks. And, we have coordinated with state agencies, the Federal Trade Commission and other interested organizations, such as the National Emergency Number Association, regarding their efforts to address and identify solutions to this problem. The Enforcement Bureau is committed to continuing to gather and analyze information about these companies' practices, their networks, their businesses, their customers, and other germane information.

In addition to our enforcement efforts, the Commission has taken affirmative steps to prevent those engaged in Caller ID spoofing for deceptive reasons from successfully accessing the personal information of telecommunications customers. In a recent Order tightening the Commission's Customer Proprietary Network Information or CPNI rules, the Commission determined that a carrier providing call history information over the phone to a customer must call the customer at the account's telephone number of record to provide such information rather than rely on Caller ID as an authentication method, thereby eliminating one of the major tools of pretexters.

As the Commission indicated in its testimony before the House of Representatives Energy and Commerce Subcommittee on Telecommunications and the Internet last year, the Commission may not have sufficient authority to fully address this issue; some of these entities do not appear to be directly regulated by the Commission, an assertion made by some targets of our investigations. Thus, legislation that clarifies the Commission's authority in this area would be helpful.

In conclusion, the intentional manipulation of Caller ID information, especially for the purpose of fraud or deception, is a troubling development in the telecommunications industry. The Commission looks forward to working with this Committee, and other Members of Congress, to ensure the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to speak with you today.

Senator NELSON. Thank you, Ms. Monteith. At any time, Senator Stevens, since you have to leave early, that you want to go ahead and ask questions, feel free.

Mr. Cerasale?

STATEMENT OF JERRY CERASALE,
SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS,
DIRECT MARKETING ASSOCIATION, INC.

Mr. CERASALE. Thank you very much, Senator Nelson, Senator Stevens, Senator Klobuchar. It's a privilege to be here today. The Direct Marking Association is a trade organization representing multi-channel and interactive marketers who use the mail, the phone, the Internet, e-mail, direct response TV, and radio to reach consumers and businesses.

Spoofing of Caller ID harms the consumer. At a minimum, it deceives the consumer. More so, it can defraud them or even put them in harm's way. Spoofing of ID also harms the company. It's actually stealing the company's identification. Stealing the ID of the company, it ruins the reputation, those actions taken by the spoofer are believed by the recipient of the phone call to be the marketer itself calling and so it harms both the consumer and the business if it's done.

We believe it also undermines the integrity and trust in this communication channel, which also is harmful to the economy, to government and so forth as we look at communications within the United States. The DMA issued guidance about spoofing a long time ago. It's attached to my written testimony.

Caller ID, properly used, helps the consumer. It let's them know who is calling, what it is and you can channel your phone calls yourself and have control over your telephone inbox. So long ago, the DMA required its members to present Caller ID, including the name of the company and send not fraudulent, truthful—sending out that information.

But to be fully useful, Caller ID has to—marketers have to be able to change Caller ID information. If I'm calling you as a telemarketer, Senator Nelson and there's the number and you want to try and get back to me, that phone number will be consistently busy because it's an outgoing telephone number.

So the idea is, we have to put in a consumer customer service number where there are people ready to respond to the call, respond to the request from the consumer, including even putting them on the company's specific Do Not Call list.

So there has to be an ability for the direct marketer to alter the Caller ID, but not for fraudulent purposes but to actually assist the consumer. Also, another problem is the duty of the marketer should be to transmit to the carrier the proper Caller ID information. We've found many times in instances that in presenting it to the consumer's phone, the information sometimes gets garbled and the marketer should not—if they have transmitted the information correctly, that should be the duty of the marketer. Now, it's no doubt when it has happened, there have been times when the number is altered when it's received by the consumer so that the local area code is placed in front of the number. And of course, the poor individual who then has that number that gets all the calls, gets angry at the marketer and eventually we find out and try and work it out quickly and communications carriers are helpful in trying to fix that and so forth; but we want to make sure that the liability on the marketer is to transmit to the carrier the proper information. That is the duty of the marketer.

Looking at S. 704, we support S. 704. We think if you added an intent to defraud or cause harm standard, you would protect the marketer, those situations that I just mentioned in the sense of changing to a customer service number, transmitting the proper number to the carrier. It also would cover, we think, some of the instances that you mentioned, Senator Nelson, concerning the police trying to protect police numbers, not showing them, centers, shelters for homeless women, battered women that calling out, you don't want to show the number of that. Put some other number in there, a social service number or something so that you can try and protect people.

Those are things, I think, that we need to try and protect in S. 704, those kinds of changes. We want to go after the spoofers, give the FCC all the authority it needs to shut these people down and we just need the ability to make Caller ID a valuable service as long as we're not using it to defraud or deceive. Thank you very much.

[The prepared statement of Mr. Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

I. Introduction & Summary

Good morning Mr. Chairman and Members of the Committee. I am Jerry Cerasale, Senior Vice President for Government Affairs of the Direct Marketing Association, and I thank you for the opportunity to appear before the Committee as it examines S. 704 and the Caller ID spoofing issue in general.

The Direct Marketing Association, Inc. ("DMA," *www.the-dma.org*) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA and our members appreciate the Committee's continued outreach to the business community on important issues such as Caller ID spoofing. DMA fully supports the efforts of Senators Nelson, McCaskill, and Snowe, and the Committee, to enact legislation prohibiting Caller ID spoofing. Spoofing is a malicious practice that undermines Caller ID as a useful verification device, and can cause harm to both consumers and business. DMA has long recognized Caller ID as an important enhancer to two-way communication between people making and receiving calls, especially in the context of business and customer relations. Caller ID provides consumers with choice and control over their telephones. It alerts a consumer as to the identity of a caller and allows the consumer to choose whether to answer a call from a marketer offering a product or service of interest.

Caller ID, when used for illegitimate purposes, can have a harmful effect on consumers and legitimate marketers and other businesses. Bad actors use Caller ID spoofing to damage a competitor's reputation, to gain unauthorized access to a consumer's personal information, and to commit illicit practices such as phishing and pretexting. The cumulative effect is consumer confusion, possible identity theft, and the transfer of ill will to legitimate businesses and marketers. We believe that spoofing, and, in general, the manipulation of Caller ID for illegitimate purposes, should be prohibited.

Understanding the importance of standards and best practices in fostering consumer choice, DMA several years ago, working with our members, developed and adopted Caller-ID Requirements as part of our Guidelines for Ethical Business Practice ("Guidelines"), to specifically discourage illegitimate telemarketing practices that threaten to undermine consumer confidence and relations with legitimate marketers.[1] In 2004, in response to a rise in Caller ID spoofing, DMA issued an advisory detailing marketers' rights and responsibilities when using Caller ID technology.[2] DMA requires its members, including nonprofits and other groups, to transmit Caller ID information. Specifically, when DMA members make marketing calls, they are required to transmit the name of the seller and the telephone number by which a called party can call back during normal business hours to ask questions or request not to receive future calls. Under our Guidelines, DMA members must not transmit a false name or telephone number.

DMA also supports the importance of accurately disclosing identity and contact information in other forms of marketing communications. For example, in the e-mail context, our Guidelines detail responsible practices for marketers to disclose accurate identifying information. The problems caused by inaccurate e-mail headers are similar to those in the Caller ID spoofing context. In 2002, in response to illegitimate actors manipulating e-mail message headers, we developed and adopted Com-

---

[1] Caller-ID/Automatic Number Identification Requirements, Article #46, DMA Guidelines for Ethical Business Practice, at 23 (attached) (available at *http://www.the-dma.org/guidelines/EthicsGuidelines.shtml*).

[2] DMA Statement Caller-ID Falsification, September 2004 (attached) (available at *http://www.thedma.org/guidelines/callerid/shtml*).

mercial Solicitations Online requirements as part of our Guidelines.[3] Our members are required to clearly disclose the marketer's identity and street address in e-mail solicitations. The identity of the sender of the message must be provided clearly, honestly, and not in a misleading manner. The subject lines must accurately convey the content of the message, and the header information must be accurate. These requirements are also part of the CAN–SPAM Act that emerged through this Committee.

II. Legislation Should Include an "Intent To Defraud or Cause Harm" Requirement

As stated at the outset, DMA supports the purpose of S. 704, to prevent the manipulation of Caller ID for fraudulent, spoofing purposes. While the practice of spoofing to defraud or cause harm to a person is unacceptable, there are legitimate reasons for transmitting Caller ID information that is different from the calling party's information that the Committee should ensure are not restricted. Blocking or modifying Caller ID information is necessary in several contexts such as safety, protecting privileged communications, and in business and customer relations. Businesses rely on the practice of modifying Caller ID for such purposes as to facilitate a consumer's request to be placed on a business's do-not-call list and to properly disclose the identity of the entity on whose behalf a third-party marketer is calling. In order to ensure that non-spoofing activities that may involve display of Caller ID information that is different from that of the entity making the call are not unintentionally covered by the legislation, we suggest that the scope of conduct covered by the legislation should be narrowed to restrict only such acts committed with "intent to defraud or cause harm."

Inclusion of such an "intent to defraud or cause harm" standard will serve the purpose of explicitly recognizing that the widely adopted business practice of transmitting a customer service telephone number in place of the calling party's telephone number is not restricted. Without such an intent standard, telemarketers that substitute a customer service telephone number for call back purposes could be covered by the bill. This practice is, in fact, currently required under existing law whereby marketers are required to transmit a telephone number through a caller identification service by which a called party may place a return call to make inquiries or request that their telephone number be added to the calling party's do-not-call list. Often businesses provide the telephone number of their customer service department to facilitate such requests rather than the number of the calling party's line. Businesses that employ such practices are not seeking to defraud or mislead customers, but rather transmitting the most relevant information and creating processes to efficiently respond to customer requests.

In addition, we are aware of scenarios where the Caller ID information transmitted from the telemarketer to a telecommunications carrier is not the same as the information provided by the carrier to the call recipient. With a strict liability standard, and with no intent standard, telemarketers could be liable for an act of the carrier over which the telemarketer has no control. Thus, the addition of an "intent to defraud or cause harm" standard also will ensure that a telemarketer is only responsible for accurately providing Caller ID information to the carrier and not for incorrect transmission by the carrier.

Requiring that a calling party provide its exact name and telephone number could jeopardize legitimate practices and restrain consumer preferences. Requiring "intent to defraud or cause harm" will ensure that bad actors with ill intent are targeted by the legislation rather than legitimate practices, customer preferences, and the underlying technology used. We believe that tying the act of transmitting misleading Caller ID information with an intent standard appropriately identifies the offending act while ensuring that businesses are not liable for simple mistakes or other instances where changing the Caller ID information is appropriate. We note that this is the approach that is in the Caller ID spoofing bills that recently passed the House of Representatives.

* * * * * * *

Thank you for your time and the opportunity to speak before your Committee. I look forward to your questions and working with the Committee on this legislation.

---

[3] Commercial Solicitations Online, Article #38, DMA Guidelines for Ethical Business Practice, at 20 (attached) (available at *http://www.the-dma.org/guidelines/EthicsGuidelines.shtml*).

EXCERPTS FROM THE DMA GUIDELINES FOR ETHICAL BUSINESS PRACTICE

Commercial Solicitations Online

Article #38

Marketers may send commercial solicitations online under the following circumstances:

- The solicitations are sent to the marketers' own customers, or
- Individuals have given their affirmative consent to the marketer to receive solicitations online, or
- Individuals did not opt out after the marketer has given notice of the opportunity to opt out from solicitations online, or
- The marketer has received assurance from the third party list provider that the individuals whose e-mail addresses appear on that list:
  - have already provided affirmative consent to receive solicitations online, or
  - have already received notice of the opportunity to have their e-mail addresses removed and have not opted out, and
- The individual is not on the marketer's in-house suppression list

Within each e-mail solicitation, marketers should furnish individuals with a notice and an Internet-based mechanism they can use to:

- Request that the marketer not send them future e-mail solicitations and
- Request that the marketer not rent, sell, or exchange their e-mail addresses for online solicitation purposes

If individuals request that their names be removed from the marketer's in-house online suppression list, then the marketer may not rent, sell, or exchange their e-mail addresses with third parties for solicitation purposes.

The above requests should be honored within 10 business days, and the marketer's opt-out mechanism should be active for at least 30 days from the date of the e-mail solicitation.

Only those marketers that rent, sell, or exchange information need to provide notice of a mechanism to opt out of information transfer to third-party marketers.

Marketers should process commercial e-mail lists obtained from third parties using DMA's E-Mail Preference Service suppression file. E–MPS need not be used on one's own *customer* lists, or when individuals have given affirmative consent to the marketer directly.

Solicitations sent via e-mail should disclose the marketer's identity and street address. The subject and "from" lines should be clear, honest, and not misleading, and the subject line should reflect the actual content of the message so that recipients understand that the e-mail is an advertisement. The header information should be accurate. A marketer should also provide specific contact information at which the individual can obtain service or information.

* * * * * * *

Caller-ID/Automatic Number Identification Requirements

Article #46

Wherever the technology is available marketers should:

- Transmit a telephone number such as the telephone number of the seller, service bureau, or customer service department that the consumer can call back during normal business hours to ask questions and/or to request not to receive future calls and
- Transmit the name of the seller or service bureau

Marketers should not block transmission of caller identification or transmit a false name or telephone number.

Telephone marketers using automatic number identification (ANI) should not rent, sell, transfer, or exchange, without customer consent, telephone numbers gained from ANI, except where a prior business relationship exists for the sale of directly related goods or services.

DMA STATEMENT CALLER-ID FALSIFICATION

Falsely altering Caller-ID information for marketing purposes is not only unethical, it is illegal!

In response to recent news reports about a new Caller ID service that would allow subscribers to transmit false Caller-ID information, The DMA has issued this statement to remind marketers about their rights and responsibilities when using Caller-ID technology.

When calling customers or prospects, it is deceptive and unlawful for a marketer to knowingly substitute and transmit a false, or 'dummy,' telephone number. Rather, wherever the technology is available, a marketer must:

- transmit the name of the seller or service bureau; and
- transmit an accurate and valid telephone number for the seller, the service bureau, or respective customer service department. A consumer should be able to call back this telephone number during normal business hours to ask questions and/or to request not to receive future calls.

Please note that a marketer MAY transmit a Caller-ID telephone number that is DIFFERENT from the number from which the call is coming AS LONG AS the number transmitted correctly identifies the name of the seller or service bureau and is a valid number that the consumer may call back during normal business hours to ask questions and/or to request not to receive future calls. For example, sometimes it may be necessary to transmit a Caller-ID number for the customer service department, instead of the number of the representative who is calling (since the representative's number will likely be busy). In this instance, substituting the customer service department number provides the consumer with a number he/she can call back for more information and/or to request to be put on the company's do-not-call list.

A marketer who intentionally creates and transmits inaccurate or false Caller-ID information is violating Federal law—for starters, the Federal Trade Commission Act (which outlaws unfair and deceptive trade practices), the Federal Trade Commission's Telemarketing Sales Rule, and the Federal Communications Commission's Telephone Consumer Protection Act.

Moreover, transmitting false Caller-ID information violates the Direct Marketing Association's Guidelines for Ethical Business Practices (*Article #44* and *Article #51*). Specifically, *Article #44* (Caller-ID/Automatic Number Identification Requirements) advises: "Marketers should not block transmission of caller identification or transmit a false name or telephone number . . ." *Article #51* (Laws, Codes, and Regulations) calls for marketers to abide by state, Federal and local laws governing marketing practices and business transactions.

Senator STEVENS. Senator, I'm going to have to leave. Could I just ask if you'd do two things. First, there is a House bill, H.R. 251 that has been passed and has been sent to the Senate. Senator Kyl has a bill, S. 1654, which has been sent to Judiciary. I think there is a criminal side of this and there is also a communications side of it. I'd appreciate it very much if you could give us, give to our staff, any suggestions you have about modifications of the bill with regard to the communications aspect so that we could have that information before the mark up next week.

I do believe we will mark up the bill and get it out next week, but I'd hope that we'd be able to make any changes that would be necessary to get it to the floor in a manner that would not be controversial. I think if you have amendments that we can consider next week, it would be very helpful. Thank you very much. I hope you'll make me a co-sponsor, Mr. Chairman.

Senator NELSON. Without objection.

Senator STEVENS. Thank you.

Senator NELSON. Thank you, Senator.

Senator STEVENS. I also have questions I'll file for the record.

Senator NELSON. OK. Thank you, Mr. Cerasale. Ms. Knight?

STATEMENT OF ALLISON KNIGHT, STAFF COUNSEL AND DIRECTOR, PRIVACY AND HUMAN RIGHTS PROJECT, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Ms. KNIGHT. Good morning. Senator Nelson, Members of the Committee, thank you for the opportunity to testify today on Caller ID spoofing and the Truth in Caller ID Act of 2007, S. 704. My name is Allison Knight and I'm Staff Counsel and Director of the Privacy and Human Rights Project at the Electronic Privacy Information Center.

I'd like to discuss two separate and important privacy interests related to the issue of Caller ID spoofing and the first is the right for call recipients to be free from pretexting and other fraud that can lead to the loss of their privacy and the threats of stalking, identity theft and harassment and we've heard from the other panelists on this issue.

The second is the rights of callers to limit the disclosure of their phone numbers in order to protect their privacy and in some cases, their safety. The Truth in Caller ID Act of 2007, S. 704, as currently drafted, does not adequately protect both of these interests. EPIC recommends that any ban on Caller ID spoofing include an intent requirement so that spoofing is only prohibited where it is clear that the person who does not provide identifying information intends to defraud or to cause harm.

EPIC recommended the inclusion of an intent requirement in testimony on a similar bill introduced in the House last year and this intent requirement was incorporated into the version of the bill that recently passed in the House that was just referred to, H.R. 251. As Mark Rotenburg, Executive Director of EPIC stated, "an intent requirement preserves the privacy rights of callers and permits legitimate uses of spoofing while outlawing fraud and harassment assisted by the technology."

We also have concerns about the provision in the Senate bill that permits law enforcement agencies to possibly misrepresent their identities in the context of telecommunications services.

Before Caller ID services were offered, telephone customers generally had the ability to control the circumstances under which their phone numbers were disclosed to other people. Many individuals have legitimate reasons to report a different number than the one presented on Caller ID. For example, a person may wish to keep his or her direct line private when making calls from within an organization. Similarly, an individual with multiple communications devices, such as a landline and a cell phone and a wireless handheld device, may want to route all returned calls to one device or a number.

Now, in some circumstances, disclosure of a person's phone number may also put his or safety at risk. Domestic violence survivors, shelters and other safe homes need to preserve the confidentiality of their phone numbers. They may need to contact abusers without exposing their location in order to arrange custody or other legitimate matters. They may also need to contact other third parties, such as businesses that have permissive privacy policies and may share collected phone numbers with lists or data brokers. In all of these situations, preserving anonymity is necessary for the caller's safety.

Caller ID blocking may seem like a viable means for allowing callers to protect their anonymity while not misleading recipients, however Caller ID blocking is not a complete solution because a caller can be identified through other means, first of all, such as the Automatic Number Identification System, which was developed for emergency services. Also, some recipients prevent blocked ID calls and indications are that the number of individuals doing this is growing. So in the case of a domestic violence survivor, attempting to safely reach a required phone number, an individual would have to use spoofing for the innocent purpose of preserving the confidentiality of his or her number.

We can't ignore the privacy interests of those who decline to accept calls from unknown numbers. If an individual has been habitually harassed by phone calls from a Caller ID-blocked number, we should not permit the harasser to use spoofing as a means to circumvent the individual's screening and I believe this is the purpose, the reason that this bill was introduced.

Caller ID spoofing can create privacy risks. Last year, EPIC brought to Congress's attention, the problem of pretexting consumers' phone records. Pretexting is a technique by which a bad actor can obtain an individual's personal information by impersonating a trusted entity. For these reasons, the practice of spoofing for the purpose of fraud or for harm should be curtailed. Preventing spoofing for harmful reasons would hold illegitimate spoofers accountable.

Spoofing Caller ID numbers can create a real risk to individuals who might be defrauded or harmed by illegitimate uses of the technology, at the same time, it's important not to punish those who may have a legitimate reason to conceal their actual phone numbers. The inclusion of an intent requirement in the Senate bill would focus the punishment on harmful and fraudulent uses of Caller ID spoofing while preserving legitimate uses of the technique.

In addition, an intent requirement would render specific exemptions, such as for law enforcement unnecessary as a legitimate law enforcement activity that employs spoofing would be protected by the requirement to show an intent to defraud or cause harm.

I'd be happy to answer any questions you have. Thank you.

[The prepared statement of Ms. Knight follows:]

PREPARED STATEMENT OF ALLISON KNIGHT, STAFF COUNSEL AND DIRECTOR, PRIVACY AND HUMAN RIGHTS PROJECT, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Chairman Inouye, Vice Chairman Stevens, and members of the Committee, thank you for the opportunity to testify today on Caller ID spoofing and the Truth in Caller ID Act of 2007, S. 704. My name is Allison Knight and I am Staff Counsel and Director of the Privacy and Human Rights Project at the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. that seeks to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and Constitutional values.

Two separate and important privacy interests meet in the issue of Caller ID spoofing. First, there is the right of callers to limit the disclosure of their phone numbers in order to protect their privacy, and in some cases, their safety. Second, there is the right for call recipients to be free from pretexting and other fraud that can lead to the loss of their privacy, and the threats of stalking, identity theft, and harassment.

The Truth in Caller ID Act of 2007, S. 704, as currently drafted does not adequately protect both interests. EPIC recommends that any ban on Caller ID spoofing

include an intent requirement, so that spoofing is only prohibited where it is clear that the person who does not provide identifying information "intends to defraud or cause harm." EPIC recommended the inclusion of an intent requirement in testimony on a similar bill introduced in the House last year,[1] and this intent requirement was incorporated into the version of bill that recently passed in the House.[2] As Marc Rotenberg, Executive Director of EPIC stated, "an intent requirement preserves the privacy rights of callers and permits legitimate uses of spoofing, while outlawing fraud and harassment assisted by the technology."[3] We also have concerns about the provision in the Senate bill that permits law enforcement agencies to possibly misrepresent their identities in the context of telecommunications services.

Telephone Customers Have Legitimate Reasons to Withhold Their Phone Numbers

The introduction of Caller ID services and the associated Automatic Number Identification (ANI) created new risks to privacy. Before these services were offered, telephone customers generally had the ability to control the circumstances under which their phone numbers were disclosed to others. In many cases, there was little need for a telephone customer to disclose a personal phone number if, for example, a person was calling a business to inquire about the cost or availability of a product or wanted information from a government agency. In other cases, there was a genuine concern that a person's safety might be at risk. For example, women at shelters who were trying to reach their children were very concerned that an abusive spouse not be able to find their location.[4]

In the context of the Internet and the offering of voice services over Internet Protocol (VoIP), there are additional concerns about the circumstances under which a person may be required to disclose their identity. The Supreme Court has repeatedly made clear that the right to be anonymous is protected by the First Amendment and also that the Internet is entitled to a high level of First Amendment protection.[5]

Many individuals have legitimate reasons to report a different number than the one presented on Caller ID. For example, a person may wish to keep her direct line private when making calls from within an organization. Such an arrangement legitimately gives call recipients a number to which they can return a call, but prevents an individual person's phone from being inundated with calls that should be routed elsewhere.

In addition to threatening a person's rights to privacy and to freedom of speech, in some circumstances disclosure of a person's phone number may also put his or her safety at risk. For example, domestic violence survivors, shelters, and other safe homes need to preserve the confidentiality of their phone numbers. They may need to contact abusers without exposing their location, in order to arrange custody or other legitimate matters. They may need to contact businesses the abuser is acquainted with, and that may share survivor information with the abuser. They may also need to contact other third parties, such as businesses that have permissive privacy policies, and thus share collected telephone numbers with list or data brokers. In all of these situations, preserving anonymity is necessary for safety.[6]

---

[1] The Truth in Caller ID Act of 2006, H.R. 5126.

[2] The intent requirement was also included in the Truth in Caller ID Act of 2007, H.R. 251. EPIC testified on this House bill on February 28, 2007, in support of the intent requirement. The Truth in Caller ID Act of 2007, H.R. 251 passed the House on June 12, 2007, and was received into the Senate and referred to the Committee on Commerce, Science, and Transportation on June 13, 2007.

[3] *H.R. 5126, the Truth in Caller ID Act of 2006: Before the Subcomm. on Telecommunications and the Internet of the H. Comm. on Energy and Commerce,* 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center). *See also, H.R. 251, the Truth in Caller ID Act of 2007: Before the Subcomm. on Telecommunications and the Internet of the H. Comm. on Energy and Commerce,* 110th Cong. (2007) (statement of Allison Knight, Director, Privacy and Human Rights Project, Electronic Privacy Information Center).

[4] Letter from National Network to End Domestic Violence to the House Committee on Energy and Commerce (May 16, 2006).

[5] *Watchtower Bible & Tract Society* v. *Village of Stratton,* 536 U.S. 150 (2002), *McIntyre* v. *Ohio Elections Commission,* 514 U.S. 334 (1995), and *Talley* v. *California*, 362 U.S. 60 (1960); *ACLU* v. *Reno*, 521 U.S. 844 (1997).

[6] *Domestic Violence and Privacy*, Electronic Privacy Information Center *http://www.epic.org/privacy/dv/*.

Caller ID Blocking Does Not Adequately Protect Privacy Interests

Caller ID blocking may seem like a viable means for allowing callers to protect their anonymity while not misleading recipients. However, Caller ID blocking is not a complete solution. One reason for this is that Caller ID is not the only way that a caller can be identified. Another system, known as Automatic Number Identification, or ANI, will still disclose a caller's identity in many situations, regardless of whether or not the caller used call blocking. This means that many businesses, emergency service providers, and anyone with a toll-free number can reliably gain the phone number of a caller, even if Caller ID is blocked. Spoofing services can protect the anonymity of a caller's ANI data when calling toll-free numbers and those entities that use ANI identification.

Some recipients prevent blocked ID calls, and indications are that the number of individuals doing this is growing. In the case of a domestic violence survivor attempting to safely reach a required phone number, an individual would have to use spoofing for the innocent purpose of preserving the confidentiality of his or her number.

We also cannot ignore the privacy interests of those who decline to accept calls from unknown numbers. If an individual has been habitually harassed by calls from a caller-blocked number, we should not permit the harasser to use spoofing as a means to circumvent the individual's screening. At the same time, it is clear that there could be prosecution for harassment whether or not additional prohibition on spoofing were enacted.[7]

Spoofing Can Create Privacy Risks

This is not to say that Caller ID spoofing is an unqualified good—far from it. Last year, EPIC brought to Congress's attention the problem of pretexting consumers' phone records.[8] Pretexting is a technique by which a bad actor can obtain an individual's personal information by impersonating a trusted entity. Pretexters have spoofed the telephone numbers of courthouses, in order to harass people for supposedly missing jury duty, threatening fines or arrest unless they turn over Social Security Numbers or other personal information.[9] Rob Douglas of *PrivacyToday.com,* with whom EPIC has worked on the pretexting issue, noted how fraudsters would use spoofing services in order to fool customers into thinking that fraudulent calls were coming from trusted sources.[10]

For these reasons, illegitimate spoofing activities should be curtailed. Law enforcement and telephone companies can retrace these calls to the originating service.[11] A spoofed number is not completely anonymous and without accountability. Preventing spoofing for harmful reasons will hold illegitimate spoofers accountable.

Intent Requirement

The inclusion of an intent requirement in the Senate bill would focus the punishment on harmful and fraudulent uses of Caller ID spoofing while preserving legitimate uses of the technique. In addition, an intent requirement would render specific exemptions for law enforcement unnecessary, as legitimate law enforcement activity that employs spoofing would be protected by the requirement to show intent to defraud or cause harm.

Significance of NSA Surveillance Program for Privacy of Call Records

Mr. Chairman, I would also like to bring to the Committee's attention our concern that the National Security Agency may have constructed a massive database of telephone toll records of American consumers. Last year, EPIC filed a complaint with the Federal Communications Commission in which we alleged that Section 222 of the Communications Act, which protects the privacy of customer record information,

---

[7] *See* 47 U.S.C. § 223; 47 U.S.C. § 227.

[8] *Protecting Consumers' Phone Records: Before the Subcomm. on Consumer Affairs, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation,* 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center). *http://www.epic.org/privacy/iei/sencomtest2806.html*; *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?: Before the H. Comm. on Energy and Commerce,* 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center) *http://www.epic.org/privacy/iei/pretext_testimony.pdf.*

[9] Sid Kirchmeyer, *Scam Alert: Courthouse Con,* AARPBulletin, May 2006, *http://www.aarp.org/bulletin/consumer/courthouse_con.html.*

[10] *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?: Before the H. Comm. on Energy and Commerce,* 109th Cong. (2006) (statement of Robert Douglas, CEO, *PrivacyToday.com*), *http://www.privacytoday.com/HC020106.htm.*

[11] Peter Svenson, *Caller ID Spoofing Becomes All Too Easy*, USA Today, Mar. 1, 2006, *http://www.usatoday.com/tech/news/2006-03-01-caller-id_x.htm.*

might have been violated.[12] We urged the Commission to undertake an investigation of this issue. In light of the ongoing controversy about the possibility that Federal privacy laws were violated, the need to pursue this investigation is clear.

We respectfully ask Members of this Committee to support EPIC's recommendation that the FCC undertake an investigation of the possibly improper disclosure of telephone toll records by the telephone companies that are subject to the privacy obligations contained in the Communications Act. If the Communications Act was violated, that should be of great concern to the Committee.

Conclusion

Spoofing Caller ID numbers can create a real risk to individuals who might be defrauded or harmed by illegitimate uses of this technology. At the same time, it is important not to punish those who may have a legitimate reason to conceal their actual telephone numbers. The inclusion of an intent requirement in the Truth in Caller ID Act of 2007 would significantly improve the bill by distinguishing between appropriate and inappropriate Caller ID spoofing.

I will be happy to answer any questions you might have at this time.

Senator NELSON. Thank you, Ms. Knight. Mr. Jones?

STATEMENT OF HON. RON JONES, COMMISSIONER, TENNESSEE REGULATORY AUTHORITY; CHAIRMAN, CONSUMER AFFAIRS COMMITTEE, NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

Mr. JONES. Thank you, Senator Nelson and members of the Committee. NARUC represents the state public utility commissions, the PUCs in all 50 states, the District of Columbia and U.S. territories with jurisdiction over telecommunications, electricity, natural gas, water and other utilities and in this capacity, the PUCs are on the frontline of consumer protection in these areas and are often the first to learn of emerging consumer concerns.

NARUC is pleased to be here in support of the enactment of Caller ID spoofing legislation. In fact, NARUC considered and passed a resolution that was adopted at our summer meeting in 2006. As has been mentioned here, Caller ID spoofing harms consumers in the areas of identity theft, credit card fraud, public safety, endangerment, law enforcement interference and other areas.

But more specifically of concern to NARUC, NARUC believes that government at all levels must be able to identify and address new and novel threats in a timely fashion to ensure the safety of consumers. Allowing the practice of Caller ID spoofing to continue may reduce consumer trust in many of the public, commercial, financial and political institutions that are relied upon by American consumers.

NARUC is pleased with the inclusion of language in S. 704, acknowledging the key role state officials play in protecting consumers through enforcement of state laws that are consistent with Federal rules. NARUC's one suggestion for change in the bill would be to strike the section limiting state action while a Federal enforcement action or proceeding is pending. Federal and state agencies can mutually benefit from revelations gleaned from concurrent investigation of violations of their respective laws and we see a great benefit in not taking cops off the beat, so to speak.

Consumer protection is and has been for a long time, a core competency of state commissions. States should not be encumbered from investigation and enforcement of violations of state law.

[12] EPIC Complaint to the Federal Communications Commission (May 16, 2006).

Caller ID spoofing is a key tool in identity theft efforts by criminals. The Federal Trade Commission reports that 10 million individuals are victims of identity theft each year and identity theft is the number one consumer complaint. Passage of the Truth in Caller ID Act of 2007 will be a huge step forward in reducing the problem of identity theft. NARUC believes it will remove a major weapon that is Caller ID spoofing from the arsenal of criminals.

Senator Nelson and members of the Committee, NARUC and its members are committed to working with you to protect consumers and we urge your swift passage of S. 704 to end the practice of Caller ID spoofing and we certainly thank you for inviting NARUC to testify before the Committee and I'd be happy to answer any questions.

[The prepared statement of Mr. Jones follows:]

PREPARED STATEMENT OF HON. RON JONES, COMMISSIONER, TENNESSEE REGULATORY AUTHORITY; CHAIRMAN, CONSUMER AFFAIRS COMMITTEE, NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

Mr. Chairman, Vice Chairman Stevens, and Members of the Committee, thank you for the opportunity to testify today on S. 704, the "Truth in Caller ID Act of 2007."

I am Ron Jones, Commissioner with the Tennessee Regulatory Authority and a member of the National Association of Regulatory Utility Commissioners (NARUC). I serve as Chairman of NARUC's Committee on Consumer Affairs. NARUC represents State public utility commissions (PUCs) in all 50 States, the District of Columbia and U.S. territories with jurisdiction over telecommunications, electricity, natural gas, water and other utilities. In this capacity, PUCs are on the frontline of consumer protection in these areas and are often the first to learn of emerging consumer concerns.

We commend you, Co-Chairman Stevens, the sponsors of this legislation Senators Nelson and Snowe, your staffs and other committee members, for addressing the issue of Caller ID fraud, otherwise known as Caller ID spoofing. Caller ID spoofing is an issue of growing concern and one of the many tools criminals can use to perpetrate fraud and steal the identities of hard-working, law-abiding Americans.

I am pleased to be here today to present NARUC's support for enactment of Caller ID spoofing legislation that would prohibit the intentional falsification of the name or number that appears on a customer's caller identification (ID) display. A resolution to this end was adopted at the NARUC Summer Meeting in 2006, which I have submitted for the record with my testimony. The resolution was adopted in response to growing consumer complaints concerning the practice of Caller ID spoofing and notes the important role state PUCs play in policing such activities.

The telecommunications industry has experienced a decade of unprecedented technological innovation bringing consumers an array of new communications devices and services. Unfortunately, with new technology often come new risks and increased opportunities criminals can exploit for their own nefarious purposes.

Previously, special equipment and knowledge was necessary to fake Caller ID information. However, the rise of new multifunctional, user friendly, Internet technologies and Voice over Internet Protocol (VoIP) has put spoofing within easy reach of scammers. All one has to do is go to a website, pay a small fee—often as low as $10—type in the number you'd like to call then input the name and number that you would like to be displayed on the call recipients Caller ID. It is as easy as that.

How is Caller ID spoofing being used and how is it harming consumers? There are several areas in which this technology is being used to harm consumers, including but certainly not limited to:

- Identity theft: Caller ID fraud is a key tool in pretexting which is the practice of obtaining personal information under false pretenses
- Criminals can falsify the home number of consumers to activate or make purchases on stolen credit cards
- Emergency calls to 911 call centers can be fabricated diverting public safety resources away from real emergencies
- Terrorists could use it to mask their true location hampering law enforcement

- An ex-spouse could use it to harass a former wife or husband who has blocked calls from their phone

Each of these examples is alone a legitimate reason to prohibit the practice of Caller ID spoofing. Taken together they provide overwhelming evidence of the need for this legislation. In our increasingly technological age, government at all levels must be able to identify and address new and novel threats in a timely fashion to ensure the safety of consumers. Allowing the practice of Caller ID spoofing to continue may reduce consumer trust in many of the public, commercial, financial and political institutions that are relied upon by American consumers.

The full extent of Caller ID spoofing is difficult to ascertain. By its very nature the goal is to disguise the true identity of the perpetrator and their motives. In many cases a consumer may not even know they were a victim of Caller ID spoofing. States, like the Federal Government, are becoming more aware of this problem and are looking to prohibit the practice.

In my home State of Tennessee, our Senate approved Caller ID spoofing legislation but it failed to pass the House. Although my state does not have a specific Caller ID spoofing law, we are collecting information and learning the extent of such fraud through our oversight of the State Do Not Call (DNC) Registry.

When a complaint regarding a DNC Registry violation is received from a consumer, the Authority initiates an investigation. If it is subsequently determined that the Caller ID information utilized in the violation was falsified, it is noted in the record. A review of 2007 Do Not Call violations found forty-two complaints that the Regulatory Authority was not able to fully investigate because the originator of the call could not be determined or contacted. This happened because the number provided to us by the Do Not Call complainant was a spoofed number and could not be traced back to the caller despite agency subpoenas for phone records of the complainant in an effort to determine the identity of the caller.

The forty-two complaints represent about 14 percent of the total Do Not Call complaints received by the Tennessee Regulatory Authority since the first of this year. While this may not sound like a large percentage, it is my belief that this number is not representative of the true scope of this problem. Regardless, each of these identified forty-two instances of Caller ID fraud is a potential crime and therefore should not be condoned.

To elaborate on the breadth of this problem, let me share with you an example of Caller ID fraud investigated by my colleagues in Nebraska. The Nebraska Public Service Commission investigated a slew of pre-recorded, automatically dialed calls on the eve of the November 2006 election. The Commission received several complaints about the politically motivated calls in the days before the election. Upon investigation, the Commission learned the numbers that appeared on the Caller ID were fraudulent and in most cases they were phone numbers that were unassigned. Even with the help of the phone companies they were unable to determine the actual source of the calls.

NARUC is pleased with the inclusion of language in S. 704 acknowledging the key role State officials play in protecting consumers through enforcement of State laws that are consistent with Federal rules. NARUC's one suggestion for change in the bill would be to strike the section limiting State action while a Federal enforcement action or proceeding is pending. Federal and State agencies can mutually benefit from revelations gleaned from concurrent investigation of violations of their respective laws. Consumer protection is a core-competency of State commissions; States should not be encumbered from investigation and enforcement of violations of State law.

As I previously stated, Caller ID spoofing is a key tool in identity theft efforts by criminals. The Federal Trade Commission reports that 10 million individuals are victims of identity theft each year and identity theft is the number one consumer complaint. Passage of the Truth in Caller ID Act of 2007 will be a big step forward in reducing the problem of identity theft. It will remove a major weapon, Caller ID spoofing, from the arsenal of criminals.

Mr. Chairman, members of the Committee, NARUC and its members are committed to working with you to protect consumers. We urge your swift passage of S. 704 to end this practice. Thank you for inviting me to testify before you and I would be happy to answer any questions.

RESOLUTION* SUPPORTING FEDERAL LEGISLATION TO COMBAT CALLER IDENTIFICATION SPOOFING

Whereas, Congress is considering legislation to prohibit the intentional falsification of the name or number that appears on a consumer's caller identification (ID) display, commonly referred to as "Caller ID spoofing"; *and*

Whereas, The Truth in Caller ID Act of 2006, H.R. 5126, would make it unlawful for a person, in connection with any telecommunications service or VoIP service, to cause any caller identification service to transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm; *and*

Whereas, The use of Internet technology to make telephone calls has made Caller ID spoofing easier; *and*

Whereas, Caller ID spoofing may be used for fraudulent or deceptive purposes which could harm consumers and lessen consumers' trust in the telecommunications industry; *and*

Whereas, Caller ID spoofing may also threaten public safety by fabricating emergency calls and thereby diverting public safety resources away from real emergencies; *and*

Whereas, The Federal Communications Commission (FCC) is attempting to address this problem through enforcement actions and coordination with the Federal Trade Commission (FTC); *and*

Whereas, The National Association of Regulatory Commissioners (NARUC) and its member states have consistently supported and encouraged consumer protection and safety issues; *now therefore be it*

Resolved, That the Board of Directors of the National Association of Regulatory Commissioners (NARUC), convened in its 2006 Summer Meetings in San Francisco, California, expresses its support for Federal legislation that would make it unlawful for a person to transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm; *and be it further*

Resolved, That NARUC is committed to working with Congress, the FCC, the FTC, and the industry on a comprehensive approach to this issue in order to educate and protect consumers from Caller ID spoofing.

Senator NELSON. Thank all of you very much. Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you, Mr. Chairman. Thank you. I'm sorry I missed the opening statements. I had another meeting and I'm the new Senator from Minnesota and I have a background that is interesting for what we're talking about today because I practiced in the telecommunications area for 13 years and worked with NARUC rather extensively, Mr. Jones, and then also was a prosecutor for 8 years and so I dealt with these issues. In fact, my claim to fame is that I got a law passed in Minnesota banning Internet phishing but I still got elected somehow.

Anyway, my focus here is on trying to solve this in a way that works. I've encountered these things before where if you do things too broadly, you can make mistakes but at the same time, I've seen the consequences of these kinds of fraud and crime, especially in the criminal areas where perpetrators might try to pretend they are someone else when they're calling. And at the same time, I was very interested in what you were saying, Ms. Knight, because when I was a prosecutor, we obviously had blocked phones and I know exactly what you mean, that more and more people don't accept blocked phone calls so when you have victims of domestic abuse or people at shelters, there must be a way to get around this. So I'm

*Sponsored by the Committees on Telecommunications and Consumer Affairs. Adopted by the NARUC Board of Directors August 2, 2006

very interested and I was talking to Senator Nelson and his staff about some kind of slight change to this so that we make sure that those things wouldn't be banned or get someone in trouble for doing that for what is really a good reason.

So my questions are, well first of all, of you, Mr. Jones about the idea of striking the section that talks about allowing state action to continue. Are there state actions that are ongoing in this area or do you have examples from around the country where people are looking into this?

Mr. JONES. Well, Senator, I'm not aware of current state actions. I know in the State of Tennessee, when we have violations of the Do Not Call Registry and we seek to determine the manner of that violation, often times that we determine that that number is a spoof call. But more importantly, what we seek to try to preserve is the ability for states, when they do take action or decide to take action, to pursue Caller ID spoofing and as such, consider legislation that they are able to do so and they are not encumbered by a prohibition in Federal law from moving forward.

Senator KLOBUCHAR. Then, Ms. Monteith, did I say your name correctly? It's easier than mine. But this is based on your prepared testimony about how the FCC has met with some of the companies, wireless and wireline and Voice over Internet Protocol companies, about the Caller ID spoofing issue. Could you talk a little bit about what they said in terms of any work that is being done to try to address the issue coming from the private sector?

Ms. MONTEITH. Our meetings with service providers were aimed at both understanding potentially how this works within the telecommunications network and also discussing with them whether or not they were getting complaints from their customers about spoofing activities. We did learn how this happens in the network, and as I mentioned, there are a variety of different ways in which a number can be spoofed.

In terms of complaints, we get complaints and I think some of the telecom carriers have gotten complaints, and they try to redress them in a variety of ways. Sometimes, as I think the Committee is aware, we've found it is difficult to determine where the spoofing is coming from. Sometimes it is couched as telemarketing. Sometimes it is harassment types of complaints and it is often times difficult to identify who is at the bottom of it.

I'm not sure I've addressed your question. I'm sorry, Senator.

Senator KLOBUCHAR. No, and I can talk to some of them, too. You know, sometimes there can be technological answers to these things because it is often like looking for a needle in a haystack, as you mentioned, to try to find the perpetrator and beyond that, I remember we dealt with this with the phishing issue. Often times people are victims and they don't know it. You didn't hear a complaint because there is some marketer and maybe they didn't respond positively so we never knew it happened. But I just wondered if you have seen that happening, if you think there is a lot more of this going on than we know of.

Ms. MONTEITH. That may be the case. In just looking at the complaint numbers that the Commission has received, we really have not seen what we would characterize as a large number of consumer complaints. For example, in 2005, we received two dozen

complaints. In 2006, roughly double that, about 60 complaints, and so far this year, around 30 complaints. Those are not large numbers of complaints when you're talking about consumers nationwide having the ability to file complaints with the FCC.

Senator KLOBUCHAR. Although some people might complain to the Attorney General's Offices in their state.

Ms. MONTEITH. Correct.

Senator KLOBUCHAR. I mean, I just remember with the phishing issue, it was clearly going on. The banks were really upset about it. Their names were being used fraudulently on these e-mails and it was going on everywhere and when someone was a victim, it was bad because they would maybe lose hundreds of thousands of dollars. But there were many victims that didn't know they were victims and I'm wondering if that's a little bit of what's going on here. I don't think I'd remember if I see some marketing firm on a Caller ID. I might not answer the phone and never even know it happened. So do you think it's possible that there is more of it going on that isn't reflected in the complaints?

Ms. MONTEITH. Yes, I do think that that's possible.

Senator KLOBUCHAR. All right, good. I just wondered, Ms. Knight, if you could just talk a little bit more about the victim angle here and the privacy angle in terms of making sure as we look at how we could couch some language on the intent and make it narrow enough that it doesn't preclude prosecution of these crimes. Sometimes it's hard to prove intent but if you have someone who is stealing money or something, it makes it a lot easier. But could you give me your thoughts on that?

Ms. KNIGHT. Sure. The language that EPIC has recommended would be including an intent to defraud or to cause harm. Another reason that we chose those two terms was that first of all, fraud would generally deal with commercial violations and would imply monetary damages and then second, harm would appropriately widen the intent requirement beyond strictly fraudulent activity to capture threats to physical safety associated with activities such stalking and domestic violence that I spoke about earlier.

Senator KLOBUCHAR. OK, thank you. Mr. Cerasale, you're the only one I didn't ask a question of, so I guess my last question will be for you. I'd asked Ms. Monteith about any efforts in the private sector of looking at this issue and I wondered if you knew of any from a technological standpoint?

Mr. CERASALE. Well, from a technological standpoint, our members—as we said, most of them do, if they are telemarketers, alter the Caller ID number that is transmitted to a customer service number where someone will answer. They keep a record of watching what kind of problems they find, problems in the final transmission of the Caller ID information to the recipient. Sometimes that can be garbled and they work with the carriers to try and fix that. They have not, at this point—there has not been, from a straight marketer's point of view, a great clamor to the DMA that this is a major problem. We are starting to hear it some from banks and so forth, similar to phishing. I think you have to look at this as telephone phishing and it starts with the banks. "Please give me your number. We have a problem with our computer system and I need this."

So those kinds of things are what we're starting to see and they tend to be a spoofing of someone with whom you have a true, strong customer relationship. With so many phone numbers on a National Do Not Call Registry, there are many consumers who do not, if they are on the registry and someone is spoofing, they don't care about that. They're just going to call. Many of those consumers don't answer the phone. So then that spoofing may occur, as you spoke about and it's not reported, because I don't respond, because I'm not supposed to be receiving telemarketing phone calls, because I'm on the list. But if I receive something from my bank or something where I have a really close relationship, those are the ones that will be answered and we're starting to hear some noise from banks on that. And it looks like it may be that banks and similar types of financial institutions are going to do the same thing they've done with phishing—we will never call you and ask you directly for your account numbers, just like we'll never send you an e-mail asking for your account numbers. And I think that's the way that we see beginning, from a marketers' standpoint, of trying to combat the spoofing of a financial institution to try and defraud.

Senator KLOBUCHAR. Well, thank you. Now, I would point out, when we embarked on this phishing adventure a few years ago in our state, I just noticed yesterday—I was reading the *Star* and *Tribune* in Minneapolis and they had just convicted someone or charged someone. So I think that I wanted to thank Senator Nelson for being out front on this with Senator Snowe.

I think just because we've seen a creeping number of complaints going up is all the more reason that you want to get at least some tools in place that law enforcement can use, knowing we don't really know what direction this will go. But at the same time, making sure that we protect the privacy interests and I believe, some of the state interests, as the witnesses pointed out. Thank you very much.

Senator NELSON. Senator Klobuchar will be added as a co-sponsor.

Senator KLOBUCHAR. Thank you.

Senator NELSON. Senator Sununu?

STATEMENT OF HON. JOHN E. SUNUNU,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator SUNUNU. Thank you, Mr. Chairman. I just have a couple of questions. First let me begin with some basic questions that Senator Stevens had and that is just viewing these things from the consumers' perspective. I guess for each of our panel members, maybe we can start with Ms. Monteith, if a consumer has concerns or is a victim of domestic abuse, or they have a complaint or concern about these kind of fraudulent activities, is there anything they can do to verify the accuracy of Caller ID information that is being presented to them through their phone system?

Ms. MONTEITH. I do not know the answer to that question, other than the information, obviously, is displayed on their customer equipment and calling back the telephone number that's displayed to attempt to verify whether or not, in fact, it's the entity that it purports to be, or checking with their telecommunications carriers and looking at their call records to determine where calls came from.

But let me look into that question and I'd be happy to get back with you.

Senator SUNUNU. Thank you. Second and more broadly, there certainly was an increase in the number of complaints from 2005 to 2006 regarding spoofing. The number went from 24 complaints to 60 complaints. This year, we're about halfway through the year. We've had 30 complaints. It certainly doesn't represent a dramatic increase and I think overall, it's a relatively modest number. So I have two basic questions. First, is that level of activity necessary to do a new piece of legislation and the second is whether or not the FTC already has the authority to deal with a good deal of the fraudulent activity.

As you know, the FCC has a responsibility and oversight for a lot of the IP and broadband voice services. So one, given the level of complaints and problems and two, given that the FCC already has some authority in this area, is there is a pressing need for new legislation and if you think that there is, what specific enforcement tools are missing that aren't available already?

Ms. MONTEITH. I can't comment on the need for legislation. I would need to let the Commissioners and the Chairman speak for themselves on that matter. I would say that the FCC would investigate any consumer complaint, regardless of the number of consumer complaints that come to us. So in fact, we're looking at the consumer complaints that have been filed with us and have taken the initiative to open investigations on this issue when it came to our attention.

Senator SUNUNU. But there's nothing restricting you from opening investigations? There's nothing restricting you from enacting penalties where fraudulent activity is found?

Ms. MONTEITH. With respect to penalties, two things, I think. One, we've already testified that it's not clear that we have the authority in this area over entities that are not directly regulated by the Commission and, in fact, that issue has been raised in response to our Letters of Inquiry by some of the targets of our investigations. And second——

Senator SUNUNU. Specifically what entities are you talking about? As a legislator, I would hope that you don't have any authority over entities that aren't—you don't specifically have jurisdiction over. In other words, we set up jurisdictional boundaries for the clear purpose of not having overlapping regulations of administration and oversight. So if there are specific entities that you believe you ought to have oversight over, you need to be specific about that, about where those gray areas might exist.

But let me—my understanding is you have oversight of telecom carriers, which has a long legal history of definition. Go ahead.

Ms. MONTEITH. That's correct. I'm talking about entities that are not directly regulated by the Commission, and not commenting on whether we ought to have jurisdiction, merely pointing out that there is a question mark that has been raised in our investigations as to whether we do have jurisdiction, since these entities are not directly regulated by the Commission and do not appear to be common carriers.

Senator SUNUNU. But with regard to those that you do have jurisdiction over, you have the ability to open cases, to carry through enforcement and to levy penalties, correct?

Ms. MONTEITH. That is correct.

Senator SUNUNU. Would the other panel members like to comment?

[No response.]

Senator SUNUNU. OK. Is there any specific enforcement tool, putting aside the issue of coverage or jurisdiction, any enforcement tool that any of the panel members want to highlight as being unavailable right now or lacking right now in current legislation?

[No response.]

Senator SUNUNU. OK, thank you, Mr.—I'm sorry, who is—it is a Chairman today? Mr. Chairman. Thank you, Mr. Chairman. I don't want any trouble there. Senator Klobuchar's chair is much larger than yours so I was entirely confused. I apologize.

[Laughter.]

Senator KLOBUCHAR. We need a visual for that to understand. Thank you.

Senator NELSON. As a matter of fact, I'm surprised that Senator Inouye and Senator Stevens allow Senator Rockefeller to have that big chair here. But because of his back, he has to have it.

Senator KLOBUCHAR. And it makes me look too small. Please continue.

Senator NELSON. I want to ask you with the fact that Voice over Internet Protocol is increasingly becoming a reality and we estimate some nine million customers today are using telephone calls through VoIP. And the fact that the FCC has jurisdiction directly over traditional telephone calls and that VoIP service providers are not clearly subject to the same FCC Caller ID regulations. So I wanted to ask any of you, do you think that this legislation plugs the hole with regard to new technologies like VoIP?

Ms. MONTEITH. Yes, it appears to do so. The only issue we might bring to your attention, Senator Nelson, is that the definition of VoIP that is crafted in the legislation does not include a provision for VoIP service that might be provided without a fee.

Senator NELSON. Without what?

Ms. MONTEITH. Without a fee. In other words, some VoIP services may be provided free of charge.

Senator NELSON. And would that not be within the jurisdiction of the FCC?

Ms. MONTEITH. Certainly not currently and in reading the legislation, I believe the legislation defines VoIP as two-way communications provided for a fee, directly to the public for a fee. There may be some services that are provided——

Senator NELSON. So if we're trying to get our hands around spoofing and we want you to have the regulatory authority, we've got to make that exception.

Ms. MONTEITH. I believe that it might be appropriate to include that language and we'd be happy to work with your staff.

Senator NELSON. OK, thank you for that recommendation. Commissioner Jones, you have stated in your testimony that some telemarketers are using spoofing to avoid the Do Not Call list enforce-

ment. Do you think that this legislation will fix that problem? And will it make the Do Not Call lists' enforcement easier for you?

Mr. JONES. Yes, sir. The legislation goes a long way in addressing that and certainly enforcement will be easier based on the penalties that are being proposed in there. But of course, that would only be honored by those who are not bad actors. But certainly, we believe that goes a long way and as I stated earlier, what we believe is that what would make it even stronger is to not prohibit the states from engaging in a concurrent investigation to the extent that state laws allow them to do so.

Senator NELSON. And you think the legislation as it is written, would prohibit the states?

Mr. JONES. From engaging in concurrent investigations, yes, sir.

Senator NELSON. OK. Are there any other tools that you see that we need on the Federal level to stop all of this practice?

Mr. JONES. Well, Senator, if I could think about that a little bit and get something back to you, I would appreciate that.

Senator NELSON. Well, while you're thinking about it, go beyond spoofing.

Mr. JONES. OK.

Senator NELSON. And are there any other telecommunications related scams that we need to examine?

Mr. JONES. Well, beyond spoofing, I think the major one, which is not strictly telecommunications but the convergence of technology with the phishing example that was given earlier, which is a form of web-based spoofing and the URL redirection that accompanies that, and that's the part of that particular effort that renders the victim unable to know that he or she has been spoofed because of the URL redirection. I think, to the extent that that technology gap is also considered to be closed, then that certainly will go a long way in stopping the spoofing in all of its forms, whether it is telecommunications through Caller ID or whether it is web-based, along with the URL redirection that accompanies that.

Senator NELSON. You all have suggested that we add the intent to defraud or cause harm. Does anybody disagree with that on the panel, if that is needed to be added to the bill?

Ms. MONTEITH. Senator Nelson, I don't know that the Commission has taken a position on that and again, I would be happy to get back to your staff on that issue, after speaking with the Chairman's Office and the Commissioner's.

Senator NELSON. Well, are there any other tools that you think that we need to consider in cracking down on this practice?

Ms. MONTEITH. No. I do not.

Senator NELSON. OK. Senator Klobuchar?

Senator KLOBUCHAR. You've been very helpful. Thank you to all four of you.

Senator NELSON. Well, thank you all. It was a very enlightening hearing and we will proceed with your suggestions as we mark up the bill next week. Thank you and the hearing is adjourned.

[Whereupon, at 11:03 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Millions of Americans use caller identification services to check the name or number of a calling party before they answer the phone. Historically, this information has been highly reliable, as attempts to provide false Caller ID information required specialized equipment and knowledge. However, with the growth of Internet-based calling technologies, the ability to send false Caller ID information has become significantly easier.

As a result, criminals have seized this opportunity. They rely on sending fraudulent Caller ID information, a practice known as spoofing, to cloak their identities. These con artists gain their victims trust by posing as financial institutions or government agencies and use that trust to deceptively obtain personal information that enables identify theft or other forms of fraud.

To combat this spoofing problem, Senators Nelson, Snowe, and McCaskill have introduced legislation S. 704, that would amend the Communications Act to explicitly prohibit the transmission of misleading or inaccurate Caller identification in connection with traditional phone as well as Voice over Internet Protocol services.

I support them in these efforts and look forward to the testimony from today's witnesses.