THE TRUTH IN CALLER ID ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

ON

H.R. 503

FEBRUARY 28, 2007

Serial No. 110–8

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

35–342 PDF WASHINGTON : 2007

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana

JOE BARTON, Texas
Ranking Minority Member
RALPH M. HALL, Texas
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
BUD ALBRIGHT, *Minority Staff Director*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

EDWARD J. MARKEY, Massachusetts, *Chairman*

MIKE DOYLE, Pennsylvania
JANE HARMAN, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
BARON P. HILL, Indiana
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR, New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
LOIS CAPPS, California
HILDA L. SOLIS, California

FRED UPTON, Michigan
Ranking Minority Member
J. DENNIS HASTERT, Illinois
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSELLA, New York
GEORGE RADANOVICH, California
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey

CONTENTS

WITNESSES

THE TRUTH IN CALLER ID ACT

WEDNESDAY, FEBRUARY 28, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
AND THE INTERNET,
Washington, DC.

The subcommittee met, pursuant to call, at 2:40 p.m., in room 2322 of the Rayburn House Office Building, Hon. Edward J. Markey (chairman of the subcommittee) presiding.

Members present: Representatives Doyle, Engel, Green, Solis, Upton, Shimkus, Walden, and Terry.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Good afternoon. I want to welcome everyone to this panel's first hearing. We have a very active agenda planned for the subcommittee, and I am pleased to be sitting next to my good friend, Fred Upton, as we begin this process. We will try to retain the same level of comedy that existed when he was chairman. I believe that is the way the telecommunications issues should be conducted.

Today we begin with legislation that was unanimously approved by the committee and the House in the last Congress when it was sponsored by former Chairman Joe Barton and my committee colleague Congressman Eliot Engel from New York. They have teamed up again this year and reintroduced the bill, and today we hope to gather updated testimony and approve the bill through the subcommittee.

This legislation addresses caller ID spoofing. Spoofing is when a caller masks or changes the caller ID information on their call in a way that disguises the true origination number of the caller. In many instances, a call recipient may be subject to pretexting through spoofing, which can lead to fraud, personal ID theft, harassment, or otherwise put the safety of the call recipient in danger.

It is important that we explore and analyze the use of spoofing to commit crimes and otherwise harm the public interest. On the other hand, lest we think that spoofing always has nefarious aims, we must recognize that there may be circumstances when a person's safety may be put in danger if their true and accurate call origination information is disclosed as well. What we see seek in caller ID policy is balance. This has been the case since we held hearings in the early 1990's on caller ID when this committee

sought to take into account emerging caller ID technology in a way that also allowed callers to block their origination number on a per call or per line basis. Technology also allowed call recipients to refuse to receive calls by anyone who is blocking their caller ID information from going through.

Last year we adjusted the legislation to ensure adequately achieved historic balance so that we look at consumer privacy and security. For instance, Members of Congress often have direct lines in their offices. In order to ensure that such lines do not become generally public and therefore remain useful to us, it may be necessary to keep such direct numbers confidential and have the outgoing caller ID information indicate a different number at which our offices can be reached to return calls. That gives the recipient a legitimate phone number to call back but keeps confidential lines private. There are many doctors, psychiatrists, lawyer, and other professionals who would similarly like to keep direct, confidential lines private in this way who have no intention of misleading anyone. In addition, there may be instances, for example, when a woman at a shelter seeks to reach her children at home when spoofing is important to safeguard someone's safety. Moreover, informants to law enforcement tip lines or whistle blowers have additional reasons for why their calling information should remain private. We should not outlaw any of these practices, and if the legislation that we are now considering needed clarification, we have now put that clarification in so that spoofing is put into context that would address those areas where the intent is to actually defraud or harass a called party. That is the goal of the legislation.

Again I want to commend my colleagues, Joe Barton and Eliot Engel, for their great work, and I now turn to recognize my good friend, the gentleman from Michigan, Mr. Upton.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. I thank the chairman, and I too look forward to working with you over the next 2 years before we get to get that gavel back over here, but take care of it. You can see that we did. In the last 12 years, a lot of chips in this thing as well worn. But I appreciate certainly your leadership and efforts to convene today's hearing and then markup a little bit later when this hearing is over. I am going to ask that my full statement be put into the record, and I am not going to give a definition of spoofing. You did a very good job. This is a bipartisan bill, and I will remind my colleagues that it passed by voice last year in the House on the House floor. Sadly, the Senate did not take it up; otherwise, it would have been a public law. And I commend Mr. Barton again and certainly my good friend, Mr. Engel, for their continued leadership on this very important issue.

Let me just convey a couple of different instances where spoofing was used, which clearly shows the need for this legislation. AARP alerted its members to a prevalence scam where spoofers get the local courthouse phone number to appear on folks' caller ID screens, and then they tell the recipients of the calls that they are judicial officials in order to get that victim's personal information, whether it be a Social Security number, driver's license, et cetera.

Other reported case involving a swat team that surrounded an apartment building after police received a call from a woman who said she was being held hostage in one of those apartments. As it turned out, it was a false alarm. Caller ID was spoofed to make it look like it was coming from that apartment, someone's idea of a bad prank. In other instances, criminals are stealing credit card numbers, getting the phone number of the actual card holder, and then using those credit cards to get unauthorized wire transfers, PIN numbers, a whole host of things that damage that individual's personal information, a real violation. And, of course, many of us are familiar with our own credit card companies which may ask us to call from home phones to authenticate and then activate that new card. And if the cards are stolen out of the mail, then criminals may be able to spoof our home phone numbers and authenticate and activate that new card from the convenience from their home or motel room or from whatever rock they might crawl under.

Unfortunately, spoofing does appear to be growing, and there is no law that protects the American public from it. This legislation, the Truth in Caller ID Act, would make it illegal. More specifically, it would make it unlawful for any person to cause any caller identification service to transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm. The unfortunate reality is that our age of information has resulted in an explosion of identify theft. And while new technologies have provided us with tremendous advancements and benefits, technology has also provided greater opportunities to criminals as well.

I look forward to hearing from our witnesses today and for the markup, and I would like to think that we could move this to the House floor soon with the leadership of the gentleman from Massachusetts . I yield back my time.

Mr. MARKEY. I thank the gentleman. The gentleman from Pittsburgh.

Mr. DOYLE. Thank you, Mr. Chairman. I think this bill has been well introduced, so in my first official action as vice chairman of your subcommittee, I will——

Mr. MARKEY. By the way, I would like to make that public announcement to all the members, that the gentleman from Pennsylvania, Mr. Doyle, is going to serve as a supremely competent and knowledgeable vice-chairman of this committee.

Mr. DOYLE. Well said, Mr. Chairman.

Mr. MARKEY. Thank you.

Mr. DOYLE. I am going to follow your lead from earlier this morning, Mr. Chairman, and waive my opening statement so we can get to our speakers.

Mr. MARKEY. Thank you. Let me then recognize the gentleman from New York, the author of this legislation, Mr. Engel.

Mr. ENGEL. Well, thank you, Mr. Chairman, and I will submit my statement to the record, but I just want to make a couple of comments.

First, thank you. I am truly honored that you are taking this bill at our first hearing and markup, and I really appreciate it. When it became clear to me about the problems of spoofing, I went over to then Chairman Barton and asked him if we could do this bill. And so we submitted the bill in the last Congress as the Barton-

Engel bill, but due to the changes, I like the way it is submitted in this Congress as the Engel-Barton bill. And I thank my good friend for cosponsoring it again this year as well as Chairman Upton for supporting it.

We held hearings on this bill last year, and the statement that you made, Mr. Chairman, and Mr. Upton's statements really capsulize what the hearings told us. The fact that there are instances where we may not want the real number to show and that there are many horror stories that we know and it can go, on and on in terms of political campaigns and trickery where people from one campaign can pretend they are calling from the opposition's campaign and do all kinds of things to get voters angry at the opposition.

So this is truly a bill whose time has come, and I am very grateful that we have tremendous consensus. And I am going to submit this, and I look forward to hearing the testimony and doing the markup with you. Thank you.

[The prepared statement of Mr. Engel follows:]

PREPARED STATEMENT OF HON. ELIOT ENGEL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. Chairman, I want to thank you for quickly scheduling this hearing. The bill before us today is a good bill and one that I was happy to re-introduce in this Congress with my friend and ranking member, Mr. Barton.

For years now, I have been working with my colleagues on issues of privacy and identity theft. Each and every time we plug one hole, crafty criminals come up with another way to commit fraud.

Currently, it is easy, cheap, and legal to spoof caller ID. These services can be used for many malicious purposes. A criminal can make a call that appears to be originating from the recipient's neighborhood bank, his credit card company, or the Social Security Administration.

I've read news reports that criminals are using these technologies to get people to give out private information they would never give out except that they think they are receiving a legitimate call from their bank or even local court house.

I also have read about some of our colleagues being victims in their capacity as Members of the House. At that point, it became apparent to me there are people who seek to use these technologies to strike at the heart of our democracy.

Leaving fake messages that are insulting or incendiary on a person's voicemail that identifies the caller as an elected official or candidate for public office threatens the very nature of our electoral process.

The Truth in Caller ID Act will give us another tool to combat identity theft and even election fraud.

I thank the chairman for his attention to this matter, look forward to hearing from the witnesses, and yield back.

Mr. MARKEY. Thank you. And, yes, this is the 20th anniversary, this month, of my becoming chairman of this subcommittee 20 years ago. So it is an honor for me to have this bill be the first bill on the 20th anniversary that we will be processing. The gentleman from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. Congratulations, and I am glad you brought up that there are some beneficial uses. I kind of forgot about when people call us on our cell phones, member to member, it is a different number that pops up on our cell phones, even in this system. So we all want to go after the bad actors, but there are some credible positive uses, and we want to maintain that balance. I think you will try to do that. I appreciate your efforts, and I yield back my time.

Mr. MARKEY. The gentle lady from California.

Ms. SOLIS. Thank you, and congratulations to you, Mr. Chairman, and also for bringing this very timely piece of legislation forward. I want to tell you that, as a longtime advocate on domestic violence issues, I am pleased to see that the legislation helps to clarify that law to protect those victims. So thank you very much, and I will submit my statement for the record.

Mr. MARKEY. The gentleman from Oregon.

Mr. WALDEN. Thank you, Mr. Chairman. I actually thought when I saw something about spoofing on our list today that it had more to do with the full committee chairman's comment about DTB yesterday and maybe changing the date. But since it is on this, I really don't have an opening statement. I supported this bill last time, and I will look forward to supporting it again.

Mr. MARKEY. The gentleman from Nebraska.

Mr. TERRY. I will waive. Happy anniversary, by the way.

Mr. MARKEY. Thank you so much. I was a young man once ago.

So let us now turn to our incredibly impressive panel of witnesses. That would be Ms. Allison Knight, staff attorney from the Electronic Privacy Information Center. She is staff counsel at that organization, a graduate of the University of Western Ontario. She has written extensively on this subject, and we appreciate very much her being here.

We have Ms. Staci Pies, who is vice-president and Point One president, testifying on behalf of the VON Coalition. She has 15 years of experience in communications, legal and regulatory experience, and she also served at the FCC as deputy division chief in a network services division, and senior attorney in the FCC's common carrier bureau.

And Ms. Kris Monteith, chief of the FCC enforcement bureau. She is the chief of that bureau. She has held numerous jobs in the FCC including overseeing the commission's interaction with local, state, and tribal governments. She has also served as the chief of policy for the wireless telecommunications bureau and deputy chief of the Farmer Common Carrier Bureau's competitive pricing division.

So I think what we will do is we will recognize the witnesses in the order that I introduced them, and then we will finish up with the FCC giving us their summary view of this issue. So, Ms. Knight, you have 5 minutes. Please begin.

STATEMENT OF ALLISON KNIGHT, STAFF COUNSEL AND DIRECTOR OF PRIVACY AND HUMAN RIGHTS PROJECT AT THE ELECTRONIC PRIVACY INFORMATION CENTER

Ms. KNIGHT. Good afternoon. Chairman Markey, Ranking Member Upton, and members of the subcommittee, thank you for the opportunity to testify today on caller ID spoofing and H.R.251, The Truth in Caller ID Act of 2007.

My name is Allison Knight, and I am staff counsel and director of privacy and human rights project at the Electronic Privacy Information Center. EPIC is a nonpartisan research organization based on Washington that seeks to focus public attention on the emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

I would like to discuss two separate and important privacy interests related to the issue of caller ID spoofing. The first 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. The second 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, identify theft, and harassment.

Before caller ID services were offered, telephone customers generally had the ability to control the circumstances under which their phone numbers were disclosed to others. Many individuals have legitimate reasons to report a different number than the one presented on caller ID, as was remarked in the opening comments. For example, a person may wish to keep their direct line private when making phone calls from within an organization. And in some circumstances, disclosure of a person's telephone number may also put his or her safety at risk. Domestic violence survivors, shelters, and other safe homes need to preserve their 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 also may need to contact other third parties, such as businesses, that may have very permissive privacy policies and would then share collected telephone numbers with lists or data brokers. In all of these situations, preserving anonymity is necessary for their 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. A caller can be identified through other means, such as the automatic number identification system, and some recipients prevent receiving blocked calls. And indications are that numbers of individuals who are 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 can't ignore the privacy interest of those who decline to accept calls from unknown numbers. If an individual has habitually received harassment 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.

Caller ID spoofing can also 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 harm should be curtailed. Preventing spoofing for harmful reasons will also 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 is important not to punish those who have a legitimate reason to conceal their actual telephone numbers.

EPIC supports H.R.251 as currently drafted because including an intent requirement, The Truth in Caller ID Act of 2007 distinguishes between appropriate and inappropriate caller ID spoofing and also preserves legitimate law enforcement techniques. Finally,

we would also like to call the subcommittee's attention to our ongoing concern about the revelation that the National Security Agency may have constructed a massive database of telephone records of American consumers. We again ask members to support EPIC's recommendation that the FCC undertake an investigation of the possibly improper disclosure telephone records by telephone companies that are subject to the privacy obligations contained in the Communications Act. Thank you.

[The prepared statement of Ms. Knight appears at the conclusion of the hearing.]

Mr. MARKEY. Thank you. Ms. Pies.

STATEMENT OF STACI PIES, VICE PRESIDENT, POINT ONE, AND PRESIDENT, THE VOICE ON THE NET COALITION

Ms. PIES. Thank you, Chairman Markey, Vice Chair Doyle, Ranking Member Upton, and members of the subcommittee. My name is Staci Pies. I am vice president of Point One, a VoIP provider, and president of the Voice on the Net or VON Coalition, the voice for the VoIP industry.

Misleading people through the misuse of caller ID, whether for a prank, a scam, or worse, is unacceptable. And on behalf of the VON Coalition, I thank the committee for its leadership in addressing this issue.

VoIP is burgeoning in popularity with businesses and consumers because it can do so much more than plain old telephone service. VoIP allows consumers to take control over the communications experience, to manage how they use those services, and to decide when and where they receive calls. Lower costs coupled with a seemingly endless list of new possibilities are making VoIP one of the hottest Internet and broadband technologies today. Today's VoIP services are simply a means to have a conversation. They are portals to a world of information that enriches the communications experience and adds new dimensions to the idea of a conversation.

Studies have shown that with the right policy framework and continued advancement, VoIP-driven competition has the potential to save consumers more than $100 billion over the next 5 years. For businesses, VoIP is lowering costs, increasing mobility, enabling collaboration, integrating voice and data in entirely new ways, boosting productivity, and giving companies and competitive advantage, and the best is yet ahead.

Many of the great benefits of VoIP to consumers and business users depends on accurate and non-misleading identification of the calling party. If I program my VoIP service to ensure that calls from my son's school are simultaneously rung on all of my phones, I don't want to answer it and find out that some telemarketer has spoofed the number to fool me into believing it is a priority call.

To protect the usefulness of their services, VoIP providers have a strong interest in having caller ID be accurate and non-misleading. The VON Coalition has been at the forefront of promoting best practices to enable consumers to protect their personal data, moving early to adopt and post consumer guidelines for protecting billing records. Since then, businesses that control personal data, consumers, and the IP industry have taken significant steps to self-police fraudulent access to personal data. The VON Coalition

agrees with previously presented congressional testimony that caller ID fraud perpetrators must be penalized. Law enforcement should have the tools to protect U.S. citizens from individuals that fraudulently manipulate phone numbers to commit a crime against a person or a crime against property. Spoofing to defraud or harass or for unlawful commercial gain cannot and should not ever be condoned or tolerated. Congress is right to focus its attention on those who would do so.

As this committee addresses deceptive spoofing, we urge you to continue to carefully balance to goal of thwarting criminal behavior with the public interest imperative to ensure that innovation flourishes and that applications and services delivered over broadband are available to all Americans. As Chairman Markey so eloquently described in his opening statement, the ability to consumers to control various aspects of their communication experience presents exciting opportunities for the disabled, offers unsurpassed privacy protection, and enables businesses and consumers to communicate in increasingly efficient and powerful ways.

The Truth in Caller ID Act, with the focus on the intent to commit fraud or other crimes, effectively balances these two important objectives by facilitating prosecution while not thwarting or prohibiting innovative tools that have legitimate consumer empowering benefits. The bill recognizes that caller identification information may be modified for telemarketers to comply with the TCPA. This is not the only legitimate need to change caller ID.

I would like to share five examples. First VoIP services offer tremendous potential for persons with disabilities to communicate more effectively. One recent Web application permits users to call any phone number in the U.S. or Canada, and the service reads to the called party the message that the originating user inputs into a Web-based form. Users of the application who are speech impaired can now send voice messages. Similarly, blind users can now take advantage of instant messaging services, where previously they would have been precluded from doing so because of sight limitations.

Second, one of the benefits of VoIP is to help consumers better protect their own privacy. For instance, Web sites that allow consumers to post solicitations for lawful commercial purposes may also permit consumers to provide a temporary callback number that is different from their assigned number. One service explains the application in this way. The desire to communicate cannot be crippled by privacy. The application unleashes the true potential of the global community by making it a safer place.

Third, as recognized by Chairman Markey and Ms. Knight, there are some situations in which caller ID information can actually endanger individual safety. The classic situation is the battered spouse. In some instances, blocking the delivery of caller ID information might be sufficient; however, because technological innovations also facilitate the unblocking of caller ID, any legislation should be careful about presuming that blocking will always be adequate protection.

Four, certain new communication services do not organically generate or transmit caller ID, but in order to connect to the public telephone network, the service may need to insert something that

looks like a traditional phone number. Many of these innovative services, which offer tremendous ways to communicate, do not utilize the same numbering and labeling practices as yesterday's phone services and should not be deemed illegitimate because of this.

A final exciting new application is the ability for consumers to make click-to-dial calls while viewing broadband-based content. Utilizing such an application, a viewer can click a single button on her standard remote and pull up a menu that offers a variety of products and services, including contacting her local member of Congress. The constituent can locate the contact information for the member's office and then click on a button that enables her to reach the office through a VoIP connection.

[The prepared statement of Ms. Pies appears at the conclusion of the hearing.]

Mr. MARKEY. Excellent job. Thank you. I appreciate it. I wanted you to get through all five of those. Ms. Monteith.

STATEMENT OF KRIS MONTIETH, CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Ms. MONTEITH. Good afternoon, Chairman Markey, Ranking Member Upton, and members of the subcommittee. Thank you for the opportunity to speak with you about the problem of caller identification spoofing.

As you know, caller ID services let customers identify who is calling them by displaying the caller's telephone number or other information 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 the telephone call 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 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. As a technical matter, caller ID spoofing happens by manipulating the data elements that travel with the phone call. Phone calls on the public switch telephone network, or the PSTN, are routed to their destinations by means of a specialized protocol called the signaling system seven, 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 tech-

nology 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 call as local law enforcement and public safety agencies to deploy their resources needlessly. Caller ID spoofing also can potentially threaten consumers. Spoofing can be used, for example, 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 has been actively 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 12 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 to the other companies and at the same time, served most of them with subpoenas to compel them to respond 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 inquiry letter seek information about the company's alleged spoofing methods, including detailed technical explanations and the types of technologies utilized, the identities of other companies that assist in providing the spoofing services, the purposes for the services, and information about subscribers, and whether the offered services can be used to spoof emergency services information or otherwise affect those critical first responders.

We continue to seek relevant information to assist us in fully understanding these issues and whether violations of the Communications Act or our rules have occurred. But our enforcement options may be limited by some of these entities who are not directly regulated by the commission. At the same time, we have held meetings with numerous industry representatives, including wire line, wireless, and voiceover Internet protocol based companies to determine the impact of caller ID spoofing on their consumers and networks.

In addition, we have coordinated closely 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 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 Congress, this committee, to ensure that the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to testify.

[The prepared statement of Ms. Montieth appears at the conclusion of the hearing.]

Mr. MARKEY. Thank you. We thank each of the witnesses. That now concludes the time for testimony by our witnesses, and now the chair will recognize himself for a question of the witnesses.

Ms. Knight, do you feel that the changes that have been made in the legislation take into account the context of the call so that now the bill goes after the bad actors without hindering legitimate uses of technology?

Ms. KNIGHT. Yes, the intent either to defraud or to cause harm adequately and rightly covers the illegitimate uses and still protects the legitimate uses of caller ID spoofing.

Mr. MARKEY. OK, great. I have no other questions. Mr. Upton.

Mr. UPTON. Do you think it addresses everything that we should in this bill?

Ms. MONTEITH. Yes, I think what would be important with respect to intent is that Congress and the committee provide as much in the way of legislative history as possible to inform the commission of the applicable standard under the intent standard.

Mr. UPTON. I have no further questions. Thank you.

Mr. MARKEY. The gentleman from New York, Mr. Engel.

Mr. ENGEL. Thank you very much, Mr. Chairman. Ms. Monteith, in your testimony, you mentioned that the commission has coordinated with state agencies regarding the efforts of the state agencies to identify solutions to this problem. Can you give some examples of what the states are doing to solve the problem?

Ms. MONTEITH. I know we have worked closely with the Florida attorney general's office and I believe with members of the Nayrook. I don't have any specific examples. We do participate with the Nayrook members on a monthly call that is aimed at addressing consumer protection types of issues. But I would be happy to get specific details to respond to your question.

Mr. ENGEL. Thank you. I appreciate that. Ms. Pies, you gave a line of good examples of the new technology, the VoIP providers. It is really exciting, and obviously many people use these things. My kids can tell you more about them than I can, but there is no standard, is that true, for VoIP providers when it comes to caller ID?

Ms. PIES. If I understand the question, you are asking whether there is an industry-wide accepted technical standard for transmission of caller ID.

Mr. ENGEL. Yes.

Ms. PIES. There are several different protocols that are used to provide VoIP services. Really depends on the type of service that is being provided, the type of network, whether or not it is connecting to the PSTN. And there are practices that some providers use. As Kris explained in her testimony, if you are connecting with the PSTN, there are different requirements in order to be able to pass. If you are utilizing SS7 base signaling, there is different information that has to be passed. Some providers where calls originate IP, rather than originating on the PSTN, as I described in my testimony, the networks do not organically generate caller ID that is what we think of in the traditional plain old telephone service world. So they may, for instance, insert a number such as 0001234 in order to allow the call to connect, but that call does not have a traditional phone number associated with it.

Mr. ENGEL. Do most programs let someone manually enter any caller ID info they want?

Ms. PIES. I can't answer whether most do or do not. What VoIP does that is so empowering for businesses and consumers is it essentially moves functionality that used to be in the hands of the large companies. So, for instance, setting up a PBX system. I can now download software and set up a PBX system from my home, and I can serve a small business straight from my home. I do not have to contract through Verizon. So the ability to do that also enables me to control some of the functionalities that the phone company would have controlled in the past, such as establishing the caller ID. I know that there are a number of consumer residential VoIP services that ask the consumer to select a phone number and fix that selection from the get-go, and the caller does not have the ability to manipulate it as they go on.

Mr. ENGEL. Is the industry working towards any standard that you know on how to handle things so that things would be uniform?

Ms. PIES. The industry is, as far as I know, and there are technical organizations and engineers that may be working on issues that I am not aware of. Establishing a caller ID so that calls look like plain old telephone service is probably not high on the priority list. Most of the industry standards that are being worked on allow the old network to communicate with the next generation network. And sort of making up a caller ID parameter so that it looks like an old phone call does not serve any beneficial purpose when the networks can talk to each other without that.

Mr. ENGEL. OK, thank you. Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman. I just want to follow up on this range. There is always unintended consequences when we move legislation, and it has struck me that we have defined that there is legitimate reasons to spoof for protection. We have been involved a lot with the 911 issue and enhanced 911 and identification of location. Is there a concern, especially VoIP, which is we are not totally deployed. We are still having issues with how someone uses the VoIP service. And they call 911. How do we know where they are at? And we are trying to push that out. Let us take someone who is spoofing legitimately to protect their location. What if they then try to make an emergency service call? Are they in the system, or are they not? Can they be identified, or can they not be identified either using traditional land line, cellular or VoIP? Is this something we need to talk through, or am I not technologically knowledgeable enough to say it is not an issue?

Ms. PIES. I would like to answer.

Mr. MARKEY. Yes.

Ms. PIES. That is a very good question, and actually the way that a VoIP caller or a cellular caller contacts the right PSAP, the correct PSAP for the location where the person is located, is there is a system called PANI or Pseudo Automatic Number Identification. And that number is input into a database or a server so that when my calls go in, for instance, I have a 202 number in my office in Maryland. My call will go into the 911 system, and because we have a very old 911 system that actually does not work very par-

ticularly efficiently, you have to fool the system to letting it believe that the call is coming from the right geographic location. So there is a Pseudo ANI that is associated then with my call that tells the PSAP that I am in Maryland as opposed to DC. So in fact, that is a legitimate spoofing capability that needs to be protected to enable the 911 call to go to the right PSAP. It is not something that needs to be prevented because both mobile calls or VoIP calls, any type of service that can be used from a different location from what a traditional phone service would be used, needs to have that sort of pseudo phone number to be able to tell the PSAP where to go and which PSAP to answer.

Mr. SHIMKUS. So no matter what number you change it to or the identification of the Pseudo ANI number will direct you to the location?

Ms. PIES. Correct.

Mr. SHIMKUS. Great. That is all I have, Mr. Chairman. I yield back.

Mr. MARKEY. The gentleman from Pennsylvania.

Mr. DOYLE. Thank you, Mr. Chairman. Ms. Monteith, first of all, it looks like this bill we have here in the subcommittee is a slam-dunk, and we appreciate your help in the process. I just thought while we have you here, I would like to have you tell us how an enforcement action happens. Walk us through it. And do you start it? Does the chairman's office start it? Tell us how it works.

Ms. MONTEITH. Sure. An enforcement action can be initiated through a number of different procedures. One may be that we would investigate an issue that comes to our attention that is troubling and may be a violation of the Communications Act. Secondly, we certainly could be asked by the chairman, other commissioners, to help to investigate issues. And thirdly, we are very often complaint-driven. A complaint is filed with the commission alleging a violation of the Communications Act, and we investigate to ensure that there is not or to determine that there is.

Once we initiate an investigation, our general fact finding process is to send letters of inquiry to the subject of our investigation, asking them to provide us with information concerning the underlying issues. They are compelled to respond. If they are a non-regulated entity, we sometimes serve a subpoena as well as issuing the formal letter of inquiry to ensure that they will respond to our inquiry. From there, if our investigation reveals that there has been a violation of the Communications Act, our general process with respect to a regulated entity is to issue what we call a notice of apparent liability. That is a finding that we believe there has been a violation, and we propose, in many instances, a forfeiture along with that finding. The entity then has an opportunity to respond to us and indicate to us that either factually or legally we do not understand the case or the facts before us, the law before us. From there, we go to a forfeiture order that may be—if we are dealing with a non-regulated entity or a entity that does not have an application or an application or a license or a permit from the commission, before we can go to the notice of apparent liability stage, we are required by statute to issue a citation. And before we could then go to the notice of apparent liability stage and impose a forfeiture or a fine, we would have to find a repeat violation by that

same entity of the same underlying Communications Act provision or our rules. So that is in essence the process.

Mr. DOYLE. When would the chairman or other commissioners get involved in an enforcement action, or do they ever?

Ms. MONTEITH. Involved with respect to asking us to investigate or involved in the investigation?

Mr. DOYLE. In the investigation.

Ms. MONTEITH. The bureau, of course, would coordinate with the chairman's office and with the commissioners to share information about our investigations. And depending upon whether the investigation is something that the bureau could handle on delegated authority or whether we had to present the item for the commission's full consideration, the commissioners may be more or less involved in the investigation.

Certainly if it is an item that is being presented to the commission for vote, the bureau would be responding to the commissioners and the chairman and the kinds of questions that they may have to assure themselves that they are, and they fully understand the facts and the laws surrounding the investigation.

Mr. DOYLE. Thank you very much. Mr. Chairman, I yield back.

Mr. MARKEY. The gentleman from Oregon.

Mr. WALDEN. Thank you, Mr. Chairman. I really don't have any questions. I think they have been well addressed and look forward to moving into the markup.

Mr. MARKEY. The gentleman from Nebraska.

Mr. TERRY. Thank you, Mr. Chairman. I only have one question. It is the same one that I asked last time, and I think we made sure that this appropriate use was protected, and that is within our teleservices industry. Two of the top three of which are headquartered in my district. So I just want to ask Kris if you could verify that from your reading that a teleservices company that uses their client's name and number as the caller ID number is an accepted practice and is not one that would be considered defrauding or harming.

Ms. MONTEITH. Yes, I believe that is correct under our rules.

Mr. TERRY. That would be our intent. Thank you.

Mr. MARKEY. With the gentleman yielding back, the time for questions by the members of the subcommittee has expired. That concludes the hearing. All members have 10 days, if they wish, to submit questions to the witnesses, and the committee clerk will notify the members as to how that process works. And without objection, this subcommittee is now adjourned. And we will now have the meeting once again. OK, so all the witnesses, if you would like, we thank you so much for your excellent testimony. And we will take a 1-minute break. We will recognize the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman, for your courtesy. Again, I apologize. I was just down the hall. I am actually trying to work with the Ecuador ambassador with an energy company, so you understand that, Mr. Chairman. But I just have some questions for Ms. Monteith. Commercial telemarketers are required to transmit accurate caller ID information that applies whether the calls are made in person or whether they are using automated calls. Is that correct?

Ms. MONTEITH. Yes, I believe so.

Mr. GREEN. OK, if a nonprofit, such as a political action committee or a political party or a 571 organization makes automated calls to voters, does the current FCC rules prohibit them from using inaccurate caller ID info if it is nonprofits or political campaigns?

Ms. MONTEITH. I don't believe exempt organizations are covered under our rules.

Mr. GREEN. OK, the committee memo agrees with that and says that there is no broad mandate however to the correct caller ID information be transmitted for non-commercial calls. That is the only thing. The draft bill we have today prohibits the sending of inaccurate caller ID info with the intent to defraud or cause harm. Does this language prohibit automated political calls with inaccurate caller ID info? Does that definition of with intent to defraud or cause harm, would that apply to non-profits or political campaigns?

Ms. MONTEITH. I would prefer to, if you don't mind, with all due respect, look at the question before I answer.

Mr. GREEN. OK, we will be glad to submit that.

Ms. MONTEITH. Thank you. I appreciate that. Mr. Chairman, generally intent to defraud is relatively clear for a standard, but when you add to it intent to cause harm, it is less clear. And I would hope that the FCC would interpret that standard, which causes harm, how much intent is needed to qualify? And so that is an open-ended, but we will submit that to you. And I know we have a markup set for this bill, and I have an amendment that will address it. But I will hold to the full committee, but I think there is some concern about that. And I want to make sure we don't have a loophole that can be done by non-profits or even political campaigns because our constituents can get mad when that caller ID is false. And whether it is me calling them or the Democratic Party or some non-profit group. And your organization has been very helpful in identifying some justified reasons for allowing callers to withhold and hide caller ID info, such as people making anonymous tips to newspapers and legitimate investigations, and also women's shelters, for example. We now have an intent standard in the bill, and I am concerned that organizations making deceptive political calls using fake caller ID information would not be covered. Is it your understanding this bill would include non-profit or political organizations?

Ms. MONTEITH. Well, I think that the standard deception is different than either fraud or to cause harm, and I think that the standard that has been articulated in the bill does clearly delineate between legitimate and illegitimate uses of spoofing.

Mr. GREEN. OK, can you think of any legitimate reason someone or some group that is making hundreds or even thousands of calls on an automated system would use a false caller ID? And this is open to anyone. I guess because I think the bill is a great bill. In fact, I know it has been both my colleague counsel Eliot and ranking member Barton, I just worry that we are leaving maybe a loophole here that we are not going to address. And we will have to come back at some future time.

Ms. MONTEITH. Well, again I think that the focus rightly is on the intent.

Mr. GREEN. OK, and not the causes harm?

Ms. MONTEITH. Well, either the intent to defraud or to cause harm.

Mr. GREEN. OK, so the intent to defraud would be the primary, and then to cause harm is actually in addition to it. You don't have to meet both tests.

Ms. MONTEITH. Right, the wording of the bill has an or. I would see to defraud as being more traditional fraud where there would be a calculable monetary damage that would be associated with it, whereas harm, I think, would be more along the lines of a physical harm to deal with some of the issues that I have read about in terms of safety.

Mr. GREEN. OK. Well, I guess the fraud issue, because if again for example, the Democratic Party is only calling Republican primary voters, what would you think that would be? Would that be intent to defraud with their caller ID not showing it is the Democratic Party?

Ms. MONTEITH. Well, again, I think that deception and fraud are two different standards. I won't try to make any kind of judgment on how the bill will eventually be interpreted; however.

Mr. GREEN. We don't want anybody to interpret it. We want to put it in the language so they don't have to.

Ms. MONTEITH. I mean I need further details on this.

Mr. GREEN. OK.

Ms. MONTEITH. At a later date, if you would like. Again, I would like to restate that EPIC does support the language either intent to defraud or to cause harm. We think that adequately makes a distinction between different uses.

Mr. GREEN. But again someone could still be using local calls just to deceive, and because defraud they are not, I mean except for maybe selling them an idea instead of a product——

Ms. MONTEITH. Well, again if that doesn't meet the language either to defraud or to cause harm, then it wouldn't be caught within the bill. And it would therefore be a legitimate use.

Ms. GREEN. OK, thank you, Mr. Chairman. Thank you again.

Mr. MARKEY. OK, and we look forward to working with the gentleman from Texas between the subcommittee and the full committee on his concerns. With that, the gentleman's time has expired. And again all time for questions by members of the subcommittee has expired, and this portion of the hearing has concluded. And we once again thank the witnesses for their excellent testimony, and we will recess for a minute while the witnesses clear the table. And our staff counsel can move into place so that we can begin a mark-up of this legislation.

[Whereupon, at 3:28 p.m., the subcommittee proceeded to other business.]

[Material submitted for inclusion in the record follows:]

I

110TH CONGRESS
1ST SESSION

H. R. 251

To amend the Communications Act of 1934 to prohibit manipulation of caller identification information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 5, 2007

Mr. ENGEL (for himself and Mr. BARTON of Texas) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To amend the Communications Act of 1934 to prohibit manipulation of caller identification information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Truth in Caller ID Act of 2007".

SEC. 2. PROHIBITION REGARDING MANIPULATION OF CALLER IDENTIFICATION INFORMATION.

Section 227 of the Communications Act of 1934 (47 U.S.C. 227) is amended—

(1) by redesignating subsections (e), (f), and (g) as subsections (f), (g), and (h), respectively; and

(2) by inserting after subsection (d) the following new subsection:

"(e) PROHIBITION ON PROVISION OF DECEPTIVE CALLER IDENTIFICATION INFORMATION.—

"(1) IN GENERAL.—It shall be unlawful for any person within the United States, 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.

"(2) PROTECTION FOR BLOCKING CALLER IDENTIFICATION INFORMATION.—Nothing in this subsection may be construed to prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information.

"(3) REGULATIONS.—Not later than 6 months after the enactment of this subsection, the Commission shall prescribe regulations to implement this subsection.

"(4) DEFINITIONS.—For purposes of this subsection:

"(A) CALLER IDENTIFICATION INFORMATION.—The term 'caller identification information' means information provided to an end user by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or VOIP service.

"(B) CALLER IDENTIFICATION SERVICE.—The term 'caller identification service' means any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or VOIP service. Such term includes automatic number identification services.

"(C) VOIP SERVICE.—The term 'VOIP service' means a service that—

"(i) provides real-time voice communications transmitted through end user equipment using TCP/IP protocol, or a successor protocol, for a fee or without a fee;

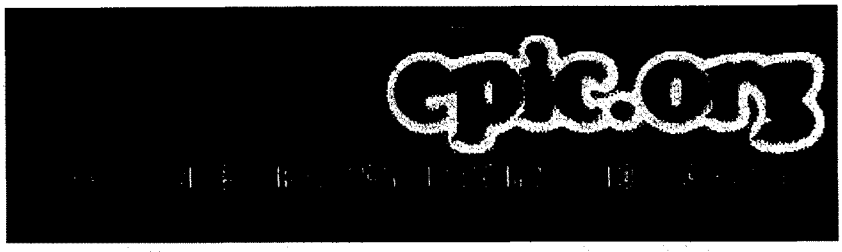
"(ii) is offered to the public, or such classes of users as to be effectively avail-

able to the public (whether part of a bundle of services or separately); and

"(iii) has the capability to originate traffic to, and terminate traffic from, the public switched telephone network.

"(5) SAVINGS PROVISION.—Nothing in this Act may be construed to affect or alter the application of the Commission's regulations regarding the requirements for transmission of caller identification information for telemarketing calls, issued pursuant to the Telephone Consumer Protection Act of 1991 (Public Law 102–243) and the amendments made by such Act.".

○



Testimony and Statement for the Record of

Allison Knight
Electronic Privacy Information Center, Staff Counsel

Hearing on

H.R. 251, the Truth in Caller ID Act of 2007

Before the

Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
February 28, 2007
2322 Rayburn House Office Building

Chairman Markey, Ranking Member Upton, and members of the subcommittee, thank you for the opportunity to testify today on caller ID spoofing and H.R. 251, the Truth in Caller ID Act of 2007. 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. Thank you for the opportunity to testify before the Subcommittee today.

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.

EPIC generally supports the approach taken to address these interests in H.R. 251. The bill as currently drafted addresses the privacy interests of both callers and call recipients by including an intent requirement in the ban on caller ID spoofing, so that spoofing is prohibited where it is clear that the person who does not provide accurate identifying information intends to defraud or cause harm. This requirement is critical to ensure that only callers with the intent to cause harm or to defraud fall within the reach of the bill.

EPIC recommended the inclusion of an intent requirement during testimony on a similar bill introduced in the House last year. 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.[1] For example, legitimate law enforcement activity that employs spoofing is preserved by the requirement to show intent to defraud or cause harm, and is therefore adequately addressed within the framework of the proposed legislation as drafted.

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.

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 already made clear that the Internet is entitled to a high level of First Amendment protection.[2]

---

[1] *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)

[2] *ACLU v. Reno*, 521 U.S. 844 (1997).

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.[3]

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-ID 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.[4]

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.[5] Pretexting is a technique by which a bad actor can obtain an individual's

---

[3] *Domestic Violence and Privacy*, Electronic Privacy Information Center http://www.epic.org/privacy/dv/.
[4] *See* 47 U.S.C. § 223; 47 U.S.C. § 227.
[5] *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

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.[6] 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.[7]

For these reasons, the practice of spoofing for the purpose of fraud or harm should be curtailed. Law enforcement and telephone companies can retrace these calls to the originating service.[8] A spoofed number is not completely anonymous and without accountability. Preventing spoofing for harmful reasons will hold illegitimate spoofers accountable.

Significance of NSA Surveillance Program for Privacy of Call Records

Mr. Chairman, as Marc Rotenberg did at the hearing last year on this issue, I would also like to call the Subcommittee's attention to our ongoing concern about the revelation that the National Security Agency may have constructed a massive database of telephone toll

---

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.

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

[7] *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.

[8] 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.

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, may have been violated. We urged the Commission to undertake an investigation of this issue.

We again ask Members 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. By including an intent requirement the revised Truth in Caller ID Act of 2007 distinguishes between appropriate and inappropriate Caller ID spooking and also preserves legitimate law enforcement techniques.

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

STATEMENT OF KRIS ANNE MONTEITH

Good morning, Chairman Markey, Ranking Member Upton, and members of the Subcommittee. 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 actively 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 twelve 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 to the other companies and, at the same time, served most of them subpoenas to compel them to respond 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 inquiry letters seek information about the companies' alleged spoofing methods, including detailed technical explanations and the types of technology utilized, the identity of other companies that assist in providing the spoofing services, the purpose for the services and information about subscribers, and whether the offered services can be used to spoof emergency services information or otherwise affect those critical first responders. We continue to seek relevant information to assist us in fully understanding these issues and whether violations of the Communications Act or our rules have occurred, but our enforcement options may be limited as some of these entities are not directly regulated by the Commission.

At the same time, we 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. In addition, we have coordinately closely with state agencies, the Federal Trade Commission and other interested organizations, such as the National Emer-

gency 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, as the Commission indicated to some members of this Committee last year, the Commission may not have sufficient authority to fully address this issue. Thus, legislation that clarified 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.

STATEMENT OF STACI L. PIES

Thank you, Chairman Markey, Vice Chair Doyle, Ranking Member Upton, and members of the subcommittee. My name is Staci Pies. I am Vice President, Governmental and

Regulatory Affairs of Point One, a VoIP provider, and President of the Voice on The Net or VON Coalition—the voice for the VoIP industry. On behalf of the VON Coalition, I thank the Subcommittee for the opportunity to testify about this important issue. Misleading people through the misuse of caller ID, whether for a prank, a scam, or worse, is unacceptable, and we thank the Committee for its leadership in addressing the issue. VoIP is burgeoning in popularity with consumers because it can do so much more than Plain Old Telephone Service. VoIP allows consumers to take control over their communications experience, to manage how they use those services and to decide when and where they want to receive calls. Lower costs, coupled with a seemingly endless list of new possibilities are making VoIP one of the hottest Internet and broadband technologies today. Internet voice communications is changing the way we communicate, stay connected to our friends, family and colleagues, and how we live. Today's VoIP services aren't simply a means to have a conversation; they're portals to a world of information that enriches the communications experience and adds new dimensions to the idea of "conversation."

Studies have shown that with the right policy framework and continued advancement, VoIP driven competition has the potential to save consumers more than $100 billion over the next 5 years. Families are gaining unprecedented independence as well as new flexibility and features not possible in yesterday's telephone network. Features such as choosing your area code, and the ability to use a VoIP service through any broadband connection are just some of the ways that consumers are benefiting. At the same time, connectivity, quality and reliability have improved to equal if not surpass that of the legacy phone network. For businesses, VoIP is lowering costs, increasing mobility, enabling collaboration, integrating voice and data in entirely new ways, boosting productivity by as much as 15 percent, and giving companies a competitive advantage.

And the best is yet ahead. The next wave of VoIP driven benefits promises to facilitate revolutionary improvements in the way we communicate. Soon a voice component can be added to any type of device, application or service that uses a microprocessor or touches the Internet. Already, making a call can be just a click away. Consumers can pay less, but get more. Communication is no longer tethered to a specific device or location. Workers can take their work phone home to spend more time with loved ones. Our armed forces can video conference with families back home—no longer having to choose between serving their families or serving their country. Free downloadable software keeps far-flung families connected, and enables children to learn a foreign language and doctors the latest medical procedures from experts around the globe. By disconnecting voice from the underlying infrastructure, voice innovation can now take place at Internet speed.

Many of the great benefits of VoIP to consumers and business users depend on accurate and non-misleading identification of the calling party. If I program my VoIP service to ensure that calls from my son's school are simultaneously rung on all of my phones, I don't want to answer it and find out that some telemarketer has spoofed the number to fool me into believing it is a priority call. And businesses that use caller ID to call up a customer's account record so that it is immediately available to the customer service representative won't find the record very useful if it is the wrong record because the caller ID has been spoofed. To protect the useful-

ness of their services, VoIP providers have a strong interest in having caller ID be accurate and nonmisleading.

The VON Coalition has been at the forefront of promoting best practices to enable consumers to protect their personal data. For instance, the Coalition moved early to adopt and post consumer guidelines for protecting billing records. Since then, businesses that control personal data, consumers, and the IP industry have taken significant steps to self police fraudulent access to personal data.

The VON Coalition agrees with previously presented Congressional testimony that callerID fraud perpetrators must be penalized. Strong action must be taken against those that intentionally spoof caller ID with the intent to commit fraud, deceive, harass or otherwise create threats to life and limb. Law enforcement should have the tools to protect U.S. citizens from criminals fraudulently manipulating phone numbers to engage in identity theft to commit financial crimes. Similarly, criminals that modify caller ID to commit other crimes, such as harassing or stalking victims, should be prosecuted swiftly and effectively. Spoofing to defraud or harass, or for unlawful commercial gain cannot and should not ever be condoned or tolerated.

Congress is right to focus its attention on those who would do so. As Congress addresses deceptive spoofing, we urge you to keep in mind that the ability to change caller ID information—where the purpose is not to fraudulently mislead or deceive—has the potential to offer consumers a transformative communications experience. Policy makers

must carefully balance the goal of thwarting harmful behavior with the public interest imperative to ensure that innovation flourishes and applications and services delivered over broadband are available to all Americans. The ability of consumers to control various aspects of their communications experience presents exciting opportunities for the disabled, offers unsurpassed privacy protection, and enables businesses and consumers to communicate in increasingly efficient and powerful ways. The "Truth in Caller ID Act of 2007" as written, effectively balances these two important objectives—by facilitating prosecution of the fraud, while not thwarting or prohibiting innovative tools that have legitimate consumer empowering benefits. The bill recognizes, for example, that law enforcement may need to mask the true identity of an originating telephone number. This is not the only legitimate need to change caller ID information. I'd like to share five examples:

• First, VoIP services offer tremendous potential for persons with disabilities to communicate more effectively. VoIP integrates the phone, voice mail, audio conferencing, e-mail, instant messaging, and Web applications on one secure, seamless network. Workers can use their PC, laptop, or handheld as a VoIP phone from virtually anywhere, with the same phone number, which benefits telecommuters, including those whose mobility is impaired and must work from home. One recent Web-based application permits users to call any phone number in the US or Canada and the service reads to the called party the message that the originating user inputs into the Web-based form. Users of the application who are speech impaired can now send voice messages simply by providing a phone number to dial and their own caller ID. Similarly, blind users can now take advantage of instant messaging services where previously they would have been precluded from doing so because of sight limitations. Importantly, the user can input her home, mobile, or office phone number, regardless of where the user is located (or where the call originates) when she sends the message, something that would be prohibited by legislation that criminalizes any change in caller ID without a reference to intent.

• Second, one of the benefits of VoIP is that it can help a consumer better protect his own privacy and manage which of his personal information he presents to the world, irrespective of which communications device he utilizes to initiate a call. Consumers may want to direct return calls to a home or business landline, rather than a wireless number, for example. Calls for different purposes (personal versus business) may merit different telephonic return addresses, as one might do with ordinary mail. For instance, Web sites that allow consumers to post solicitations for lawful commercial purposes may also permit consumers to provide a temporary call back number that is different from their assigned caller ID. This beneficial privacy service may require a legitimate change in caller ID. One service explains the application in this way: "The desire to communicate can not be crippled by concerns about privacy. [This application] unleashes the true potential of a global community by making it a safer place." While these applications manipulate caller ID, they do so for privacy protection and security. The VON Coalition does not sanction masquerading as another for fraudulent or deceitful purposes.

• Third, there are some situations in which caller ID information can endanger individual safety. The classic situation is the battered spouse. In some instances, blocking the delivery of caller ID information might be sufficient. However, because

technological innovations permit users to "unblock" caller ID, any legislation, as well as law enforcement authorities, should be careful about presuming that blocking will always be adequate.

• Fourth, certain new communication services do not organically generate or transmit a traditional caller ID, but in order to connect to the public telephone network, the service may need to insert something that looks like a traditional phone number. Many of these innovative services, which offer tremendous new ways to communicate, do not utilize the same numbering and labeling practices as yesterday's phone services and should not be deemed illegitimate simply because the technology permits the caller ID to be changed. Users without traditional telephone numbers, users with several numbers, users wanting to move numbers to their calling device and network of choice—these users are all potentially affected by technology that decouples devices from the caller ID that effectively used to be the address of the phone, and such users do not intend to defraud or cause harm. H.R. 251 appropriately focuses on the right class of services.

• A final, exciting application that I will share with you today is the ability for consumers to make click to dial calls while viewing broadband-based content such as IP-TV. Utilizing such an application, a viewer can click a single button on his standard TV remote control and pull up a menu that offers a variety of products and services—ranging from news, games, fantasy sports scores, traffic, shopping, and entertainment, to billing applications. From there, the viewer can locate a business of interest in the area and can then click on a button that enables the viewer to speak to the local business through a VoIP connection. Although the call technically originates through the VoIP service provider, the viewer can input his own caller ID for call-back purposes. Such innovative and rich communications experiences should not be eliminated through overly broad legislation or regulation.

I'd like to close with three additional thoughts. First, spoofing of caller ID is not new. Tools have been widely available for years to spoof caller ID on traditional networks. One method, sometimes referred to as Orangeboxing, offers the ability to spoof caller ID using a downloadable sound and a common tape recorder. Moreover, many large businesses operating a PBX system have, for quite some time, "spoofed" caller ID so that it appears as if all calls originating on the PBX come from the same central number. Second, fighting fraudulent and deceptive changes in caller ID is only part of the solution. Companies handling sensitive customer information must also make sure they are handling that information with care. While caller ID can help a business retrieve a customer's account record, as long as caller ID can technically be spoofed (which will be the case even with new legislation) the business needs to handle disclosure of those records with the utmost care—making consumer privacy their top priority. One security expert explained the technology is not to blame for the fraudulent use. Society is. Society has grown far too reliant on caller ID as a form of identification. Both individuals and corporate America use caller ID to decide whom to trust. Unfortunately, too many individuals have suffered because of this misplaced trust. As Chairman Dingell and Ranking Member Barton recognized in introducing "The Prevention of Fraudulent Access to Phone Records Act" to prohibit pretexting of phone records and to enhance security requirements for customer proprietary network information, it is incumbent upon companies that are entrusted with personal information to do more to protect the privacy and security of their customers.

Third, misleading people through the misuse of caller ID, whether for a prank, a scam, or worse, is unacceptable. This committee is right to focus on those who intend to mislead. At the same time, though, legislation should not impose liability on traditional carriers and VoIP services providers who merely transmit what may turn out to be fraudulently altered caller ID information. Policy makers should not be mislead into believing that technology innovators are to blame for criminal behavior. Networks and network service providers may be unable and should not be required to become "content police" or to discern legitimate and illegitimate uses of network services. Instead, service providers are best able to assist in the efforts to fight spoofing by keeping accurate records and making those records available, as appropriate, to proper authorities.

In focusing on those few people who would abuse caller ID technology, Congress can address the very real problem of deceptive spoofing effectively, in a cost-efficient manner that protects the proper use of this technology, and enables competitive and transformative innovation. VoIP service providers, who have made real strides in leveraging the power of the Internet and caller ID to provide robust services to consumers, fully support measures to protect the integrity of caller ID functionality. Together with this Committee's efforts, the proliferation of VoIP services will create unsurpassed opportunities for consumers and even greater growth in broadband services. The VON Coalition believes that VoIP is positioned to help make commu-

nicating more affordable, businesses more productive, jobs more plentiful, the Internet more valuable, and Americans more safe and secure.

Thank you very much. I am happy to answer any questions.