# H.R. 5126, THE TRUTH IN CALLER ID ACT OF 2006

## HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 18, 2006

## Serial No. 109-92

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

29-451PDF WASHINGTON : 2006

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

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
*Vice Chairman*
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
*Vice Chairman*
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
*Ranking Member*
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
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
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

---

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
JOHN SULLIVAN, Oklahoma
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
*(EX OFFICIO)*

EDWARD J. MARKEY, Massachusetts
*Ranking Member*
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
MIKE DOYLE, Pennsylvania
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
JOHN D. DINGELL, Michigan
*(EX OFFICIO)*

# CONTENTS

# H.R. 5126, THE TRUTH IN CALLER ID ACT OF 2006

**THURSDAY, MAY 18, 2006**

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

The Subcommittee met, pursuant to notice, at 9:09 a.m., in room 2123 of the Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Shimkus, Terry, Barton (ex officio), Markey, Engel, and Inslee.

Staff present: Kelly Cole, Counsel; Jaylyn Jensen, Senior Legislative Analyst; Howard Waltzman, Chief Counsel for Telecommunications; Anh Nguyen, Legislative Clerk; Johanna Shelton, Minority Counsel; and Peter Filon, Minority Counsel.

MR. UPTON. The witnesses can take their respective chairs. Good morning. Now, there was a comment on the floor last night--or I should say this morning, that another vote on a certain issue will take place tomorrow. I said, it is tomorrow. For those of you that were watching C-SPAN, most of us did not get home from votes on the budget until pretty close to 2:00 a.m., and I actually thought this hearing was starting at 10:00, but I saw that it was at 9:00. And I may be the only Member here this morning for the hearing, although I do understand that Mr. Shimkus is at a breakfast. I hope they have a lot of coffee. I understand that Mr. Engel is en route. I understand that Mr. Markey is en route, but I know Mr. Markey well, and there is a stop at Starbucks that he never fails to make, so we will see if they have a long line or not with this hearing.

But I am going to make a unanimous consent--and I did see Mr. Chairman Barton. He gave me a big smile, and he said he would be here, but I also know that he has been under the weather and under some medical assistance with vertigo, and it caused him to not get back from Texas until late yesterday afternoon. So we are going to start. I will make a unanimous consent that all Member statements will be made part of the record without a problem. And I will speak slowly, hoping that Mr. Engel will get here as his office is just down the hallway.

But anyway, today's hearing--I am going to have one more slug of coffee, it has not kicked in yet--is on H.R. 5126, the Truth in Caller ID

Act of 2006, bipartisan legislation introduced by Chairman Barton and Eliot Engel, and I commend both for their leadership. I am delighted to be a proud cosponsor of the legislation. Caller ID "spoofing" occurs when a caller fakes his caller ID information, so that the number which appears on the recipient's caller ID screen is not the caller's actual phone number. In many cases, such "spoofers" are actually transmitting someone else's caller ID information instead of their own. Apparently, some "spoofers" just do it to play practical jokes on their friends, but, in fact, there have been reports of much more sinister uses of "spoofing".

In some instances, "spoofing" is being used to trick people into thinking the person on the other end of the line is someone from a government agency, or some other presumably trustworthy party. For instance, in this month's AARP Bulletin, there is a consumer alert describing a prevalent scam where spoofers get the local courthouse's phone number to pop up on people's caller ID screens, and then they tell the recipients of the calls that they are judicial officials in order to get the unsuspecting victims to divulge personal information, like Social Security numbers, driver's license numbers, et cetera, while enforcement officials are particularly concerned about senior citizens' susceptibility to such scams.

Another important case involved a SWAT team that surrounded an apartment building after police received a call from a woman who said she was being held hostage in an apartment. As it turned out, it was a false alarm--caller ID was "spoofed" to make it look like it was coming from the apartment. Apparently, it was somebody else's idea of a bad prank.

In other instances, criminals are stealing credit card numbers, getting the phone number of the actual cardholder, and then using those credit cards to use to get unauthorized wire transfers. In such cases, the criminal "spoofs" his caller ID information so that the number which pops up on the wire transfer operator's screen is that of the actual cardholder. Because such caller ID information matches the actual cardholder's phone number on record with the credit card company, the wire transfer company uses it to authorize the wire transfer. Thus "spoofing" enables the crime to be consummated.

And, of course, many of us are familiar with our own credit card companies which may ask us to call from our home phone to authenticate and activate those new cards. If the new card is stolen out of the mail, then criminals may be able to "spoof" our home phone numbers and authenticate and activate our new cards from the convenience of their own homes, or motel rooms, or from whatever rock they might decide to crawl under.

While such "spoofing" has been technically possible for some time, it used to require specific phone connections and expensive equipment. However, with the advent of VoIP, Voice over Internet Protocol, it has become easier for callers to transmit any caller ID information that the caller might choose. Moreover, there are online companies which offer "spoofing" services for just a few bucks to anyone with a phone.

Unfortunately, nefarious uses of "spoofing" appear to be proliferating, and there is no law that actually protects the American public from it. The Truth in Caller ID Act of 2006 would make "spoofing" 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--other than for authorized activities of law enforcement agencies--and require the FCC to issue implementing regulations within six months of enactment.

Today we will hear from our witnesses about the problems of "spoofing" and their suggestions about how this bill, the Truth in Caller ID Act of 2006, might be improved. I look forward to hearing from our witnesses. I appreciate you being here on time, and also my colleague from Nebraska being on time. Mr. Terry, would you like to make an opening statement?

[The prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF THE HON. FRED UPTON, CHAIRMAN, SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

Good morning. Today's hearing is on H.R. 5126, the *Truth in Caller ID Act of 2006*, bipartisan legislation introduced by Chairman Barton and Elliot Engel, who I commend for their leadership. I am a proud cosponsor of their bill.

Caller ID "spoofing" occurs when a caller fakes his caller ID information, so that the number which appears on a recipient's caller ID screen is NOT the caller's actual phone number. In many cases, such "spoofers" are actually transmitting someone else's caller ID information instead of their own.

Apparently, some "spoofers" just do it to play practical jokes on their friends. But there have been reports of much more sinister uses of "spoofing".

In some instances, "spoofing" is being used to trick people into thinking the person on the other end of the line is someone from a government agency -- or some other presumably trustworthy party. For instance, in this month's *AARP Bulletin* there is a consumer alert describing a prevalent scam whereby "spoofers" get the local courthouse's phone number to pop-up on peoples' caller ID screens and then tell the recipients of the calls that they are judicial officials in order to get unsuspecting victims to divulge personal information, like Social Security numbers and drivers license numbers. Law enforcement officials are particularly concerned about senior citizens' susceptibility to such scams.

Another reported case involved a SWAT team surrounding an apartment building after police received a call from a woman who said she was being held hostage in an apartment. As it turned out, it was a false alarm -- caller ID was "spoofed" to make it look like it was coming from that apartment. Apparently, it was someone's idea of a bad prank.

In other instances, criminals are stealing credit card numbers, getting the phone number of the actual cardholder, and then using those credit cards to get unauthorized wire transfers. In such cases, the criminal "spoofs" his caller ID information so that the number which pops-up on the wire transfer company operator's screen is that of the actual card holder's. Because such caller ID information matches the actual card holder's phone number on record with the credit card company, the wire transfer company uses it to authorize the wire transfer. Thus, "spoofing" enables the crime to be consummated.

And, of course, many of us are familiar with our own credit card companies which may ask us to call from our home phones to authenticate and activate our new cards. If our new cards are stolen out of the mail, then criminals may be able to "spoof" our home phone numbers and authenticate and activate our new cards from the convenience of their own homes or motel rooms -- or from whatever rock they crawl under.

While such "spoofing" has been technically possible for some time, it used to require specific phone connections and expensive equipment. However, with the advent of VoIP, it has become easier for callers to transmit any caller ID information that the caller chooses. Moreover, there are online companies which offer "spoofing" services for a few bucks to anyone with any phone.

Unfortunately, nefarious uses of "spoofing" appear to be proliferating, and there is no law protecting the American public from it. The *Truth in Caller ID Act of 2006* would make "spoofing" 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 – other than for authorized activities of law enforcement agencies -- and require the FCC to issue implementing regulations within six months of enactment.

Today, we will hear from out witnesses about the problem of "spoofing" and their suggestions about how the *Truth In Caller ID Act of 2006* might be improved. I look forward to hearing from our witnesses today, and I appreciate them being here with us.

MR. TERRY. Thank you, Mr. Chairman. And I--not necessarily on time by Michigan and Nebraska standards, but getting here at 10 after in D.C. is actually early for a meeting.

MR. UPTON. I gave a long-winded opening statement just so that you could get here.

MR. TERRY. Thank you. And I do appreciate you having this hearing, and it will be interesting to hear from the panel regarding the Truth in Caller ID Act of 2006. Needless to say, coming from Omaha, Nebraska, where I represent 30,000 people in the telecommunications/tele-services business, I am concerned about how this Act may affect those companies and their employees. Many Fortune 500 companies use the tele-services in my hometown and my district in lieu of their own call centers and tele-services, so when they make an outbound call or an inbound call, they answer it, representing their claim, XYZ company. That is not "spoofing" in my mind. That is not fraudulent. That is their client and they should have a right to be able to speak on behalf of their client. So hopefully there is nothing in the Truth in Caller ID Act that prevents legitimate tele-services from doing their job on behalf of their clients. It is not fraudulent.

So I think we need to kind of work through the details here, and that is why it is important that we have this type of a hearing. And I want to thank our panels for being here today to help us work through the issues of what is legitimate, what is fraudulent. None of us want people to be able to fake identities, "spoof," in order to make contact. But on the other hand, we do not want to stop legitimate commerce as well.

With that, Chairman, I thank you for holding this hearing, and I yield back the remainder of my time.

MR. UPTON. I thank the gentleman for being here. And at this point, I make a unanimous consent request that all Members will have their opening statements as part of the record.

[Additional Statements for the record follow:]

PREPARED STATEMENT OF THE HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman.

Just like our hearing on pretexting a few months back, I'm again shocked about how people have conceived such a malevolent business model that appears to be legal. The act of "spoofing," or changing, one's caller ID information appears to be on the rise, which has dangerous ramifications for those who rely on call restrictions to protect themselves from estranged spouses or others who may be harassing them.

Now I've learned about a website that not only offers the ability to "spoof" one's caller ID, but also offers tools to change your voice and record the conversation. What legitimate business use can one imagine for these features?

We need to make certain that when someone receives a call, they can trust the caller ID information is accurate. That's why I commend Chairman Barton for his leadership on this bill and wish to join as a cosponsor to ensure the caller ID is truthful.

I yield back the balance of my time.

PREPARED STATEMENT OF THE HON. PAUL E. GILLMOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Thank you for holding this important hearing. I also would like to commend the full committee chairman, Chairman Barton, on his leadership with this important piece of consumer protection legislation.

Mr. Chairman, the issue of "Caller ID" Spoofing is not a matter to be taken lightly. Rather, it is an issue critical to ensuring the safety and privacy of our constituents. In a rapidly changing telecommunications environment, Chairman Barton's bill is a simple and straight-forward way in addressing the need to provide accurate caller ID information.

As an advocate for strong sex offender laws, I fear that erroneous caller ID information may be utilized as another tool for predators to locate their prey's location and personal information. Additionally, as a member of the Financial Services Committee, I hear all too often about how cases of identity theft have decimated an individual's financial wellbeing. If not prevented, this too could become a tool for identity thieves to deprive innocent victims of their nest eggs—especially in areas, such as my northwest Ohio district, that have a large concentration of elderly residents.

Mr. Chairman, this is an important issue that must be addressed, and I applaud you, Chairman Barton, and Mr. Engel for not allowing it to become lost as we deal with

larger, more comprehensive telecommunications reform issues. Finally, I look forward to hearing the testimony from today's panel, and to working with you and Chairman Barton to see that all of our constituents are properly protected from the dangers posed by caller ID spoofing.

PREPARED STATEMENT OF THE HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Good Morning. I want to commend Chairman Upton for calling this hearing today on legislation addressing "caller ID spoofing".

"Spoofing" is when a caller masks or changes the caller ID information of their call in a way that disguises the true origination number of the caller. In many instances, a call recipient may be subject to pre-texting 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. (We spent time earlier this year on legislation addressing these important issues, which disappeared into an intelligence-gathering black hole just before it reached the House floor, but perhaps it will re-emerge soon…..) 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 seek in caller ID policy is balance. This has been the case since we held hearings in the early 1990s on caller ID, where this Subcommittee 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 was blocking their caller ID information from going through.

While I believe the intent of the legislation before us today has a noble objective, I do not yet believe it adequately strikes the historic balance we have sought to achieve for 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 out-going caller ID information indicate a different number at which our offices can be reached for return calls. That gives the recipient a legitimate phone number to call back, but keeps confidential lines private.

There are many doctors, psychiatrists, lawyers, 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, when spoofing is important to safeguard someone's safety. Moreover, informants to law enforcement tip lines or whistleblowers have additional reasons for why their calling information should remain private. We should not outlaw any of these practices and I think the legislation needs some improvement and clarification in these areas.

Finally, I don't think the Subcommittee can convene here today and discuss spoofing, consumer privacy, and caller ID legislation without addressing the elephant in the back of the room.

We passed a bill addressing consumer phone records unanimously through this Committee earlier this Spring after due deliberation and public hearings. That legislation was pulled from the House floor apparently because intelligence entities sought changes to it. With the recent revelations about the alleged program at the National Security Agency to gather up the phone records of tens of millions of Americans, I think this Committee needs to investigate those issues in a timely manner as well and I hope the Chairman will announce such hearing soon.

Again, I thank Chairman Upton for calling today's hearing and look forward to working with him and our other colleagues on this bill as we move forward.

MR. UPTON. We have four very good witnesses today: Mr. Tom Navin, the Wireline Bureau Chief of the FCC; Ms. Staci Pies, Vice President of PointOne Communications in Texas, on behalf of Voice on the Net Coalition; Mr. Lance James, Chief Technology Officer of Secure Science Corporation; and Mr. Mark Rotenberg, Executive Director of Electronic Privacy Information Center here in Washington. We thank you all for being here this morning. And before I yield the time, Mr. Engel has just made it through the threshold for an opening statement. Again, I complemented you on being an original sponsor of the bill with Mr. Barton. I appreciate you being here.

MR. ENGEL. Thank you. Thank you, Mr. Chairman. Yes, I am a poor substitute for Mr. Markey today, but I want to thank you for quickly scheduling this hearing. I really, as you know, have worked really closely with you, and I think you have been an exemplary Chairman, and I have no problem saying that publicly and privately as well.

I support this bill obviously to combat caller ID fraud, since I have added my name as the primary co-sponsor. When we were finding out about these things, you and I had had much discussion about it as I have with Jim Gordon, and this really seemed like a no-brainer, this legislation, that really should be supported by everyone in this Congress. I also strongly support regular procedure, our colleagues are due the opportunity to learn about the issue as well, and provide their own input. The bill is a good bill. We need to continue to work to improve it, and I think that we will do that, working across party lines.

I have been working with my colleagues for years now on issues of privacy and identity theft. On each and every time we plug one hole, crafty criminals come up with another way to commit fraud. Recently on television, I was asked how come we cannot stay ahead of the curve with getting the bad guys. And I said, well, you know, the problem with this is they have to commit the fraud, and then we realize the things that they are doing, and we always sort of play catch-up with them. I have read news reports that criminals are using these technologies to get people to give out private information that they would never give out, except that they think they are receiving a legitimate call from their bank, or a hospital, or even a local courthouse, or even Congress. I have also read about our colleague Tim Murphy being a victim in his capacity as a Member of Congress, and that I heard that our colleague and committee member Heather Wilson has also been a victim.

At this point, it became apparent to me that there are people who seek to use these technologies to strike at the heart of our democracy. They could well be planning to interfere with elections. That is an

assault on the democratic process, obviously. Leaving fake messages that are insulting or incendiary on a public person's voice mail that identifies the caller as an elected official or candidate for public office can threaten the very nature of our electoral process, and we can see how it could be used politically to try to change or subvert the electoral process.

We have struggled to clean up our campaigns with greater disclosure and bans on soft money. We should not let that hard work be destroyed by a few unscrupulous acts. So the Truth in Caller ID Act will give us another tool to use to combat identity theft and even election fraud.

I thank the Chairman for his attention to this matter, and I would like to ask unanimous consent to enter into the record a letter from the National Network to End Domestic Violence. Protecting victims of domestic violence has been a major issue for this Congress, and I agree with them that the Truth in Caller ID Act must not cause us to backtrack. So I ask unanimous consent for that.

MR. UPTON. Without objection.

[The information follows:]


660 Pennsylvania Ave., S.E. Suite 303, Washington, DC 20003 Phone: (202) 543-5566 Fax: (202) 543-5626

May 16, 2006

**RE: H.R. 5126 'Truth in Caller ID Act of 2006'**

The Honorable Joe Barton
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Dingell
Ranking Member
Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

cc: The Honorable Fred Upton and The Honorable Edward Markey

Dear Chairman Barton and Ranking Member Dingell,

The National Network to End Domestic Violence (NNEDV) greatly appreciates your efforts to address impersonation through Caller Identification (ID) devices. The misuse of technology by domestic abusers and other criminals is an important issue and NNEDV would be honored to work with the House Committee on Energy and Commerce to address Caller ID spoofing in a manner that also protects the safety of victims of domestic violence and stalking.

NNEDV is a membership organization representing 53 state domestic violence coalitions, who in turn represent over 3,000 local domestic violence service providers across the country. The Safety Net project at NNEDV is the only national initiative addressing the intersection of domestic violence and all forms of technology. Safety Net tracks emerging technology issues and their impact on victim safety, working with local, State and Federal agencies to amend or create policies that enhance victim safety and confidentiality.

Batterers often misuse technology, including Caller ID, to stalk their victims. Because of this, victims of domestic violence and the service providers who assist them must sometimes provide alternate Caller ID information to shield their confidential location. It is thus critical to protect citizens from harmful Caller ID impersonation while ensuring that individuals who are merely protecting themselves are not unfairly penalized by new legislation.

Since Caller ID became available in the United States over ten years ago, phone companies have allowed individuals to block their phone number from appearing in a Caller ID device. Many local victim advocacy programs use this feature to block Caller ID for outgoing calls to increase the safety of victims, as abusers may become more dangerous if they see a domestic violence shelter name in the Caller ID device. This is important because many victims seek help while they are still living with the abusers, and

the service provider must be able to return the victims' calls without placing them in greater jeopardy. Since many phones are configured to not accept blocked or private calls, some local domestic violence shelter programs sign up for service under an affiliated name such as the United Way. Under a broad attempt to address the misuse of Caller ID information, it could be argued that these shelters are providing misleading information when in reality they are trying to protect the safety of victims of domestic violence.

Individual victims of domestic violence and stalking may also need to provide alternate Caller ID information. Internet-based phone services, also known as Voice Over Internet Protocol (VOIP), can impact Caller ID in a manner that endangers victims. Intersecting technologies often remove the protections that prevent a blocked phone number from being displayed when calling a VOIP subscriber. This phenomenon could allow an abuser who subscribes to VOIP to see the blocked phone number of a victim or a shelter. Given this development, individual victims who must call an abuser but must also keep their location secret may need the Caller ID device to display alternative information to protect their safety.

NNEDV recommends that legislation to address impersonation through Caller ID devices be more narrowly focused on prohibiting the transmission of misleading or inaccurate Caller ID information with the intent to cause harm, the intent to commit a crime, or in violation of local, State and Federal law. Addressing harmful impersonation through this focus would allow criminals to be held accountable, without inadvertently impacting victims of domestic violence and stalking and the advocacy organizations that support them.

NNEDV applauds your efforts to prevent criminals and abusers from misusing Caller Identification services to impersonate others, and looks forward to working with the Committee on this issue.

Respectfully submitted,

Cindy Southworth, MSW
Director of the Safety Net Project
National Network to End Domestic Violence

2

MR. ENGEL. I thank you, Mr. Chairman. I thank you for your attention, and look forward to hearing from the witnesses, and yield back.

[The prepared statement of Hon. Eliot Engel follows:]

PREPARED STATEMENT OF THE 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. Obviously, I support this bill to combat Caller ID fraud – since I have added my name as the primary cosponsor.

But, I also strongly support regular procedure. Our colleagues are due the opportunity to learn about the issue as well and provide their own input.

The bill before us today is a good bill but I believe there is room for improvement. Working together, across party lines, will make this a better bill.

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.

I've read news reports that criminals are using these technologies to get people to give out private information that 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 our colleague Tim Murphy being a victim in his capacity as a Member of the House. Then I learned our colleague Heather Wilson has also been a victim.

At that point it became apparent to me that there are people who seek to use these technologies to strike at the heart of our democracy. They could well be planning to interfere with elections. That is an assault on the democratic process.

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.

We have struggled to clean up our campaigns with greater disclosure and bans on soft money. We should not let that hard work be destroyed by a few unscrupulous actors.

The Truth in Caller ID Act will give us another tool to use 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. UPTON. The gentleman yields back. Again, I thank you for your leadership on this issue, and I look forward to working with you, as well as with Chairman Barton in moving this legislation quickly through our Committee and to the floor. And with that, I recognize the distinguished Chairman of the Full Committee, Mr. Barton.

CHAIRMAN BARTON. Thank you, Chairman Upton, for calling this hearing today on H.R. 5126, the Truth in Caller ID Act of 2006, introduced by myself and Congressman Engel. This bill is necessary to shut down the growing problem of manipulating caller ID information. Caller ID so-called spoofing occurs when a caller masquerades as someone else by falsifying the number that appears on the recipient's caller ID display.

Everyone is familiar with the caller ID product that provides to a consumer the name and number of who is placing an incoming call. Unfortunately, caller ID "spoofing" is yet another tool available to criminals to hijack the identities of consumers. For instance, the AARP

recently ran a "scam alert" when someone posing to be a courthouse employee called a Sterling, Michigan woman claiming that she had missed jury duty that week. The caller threatened that a warrant was being issued for her arrest, and then asked to confirm her Social Security number to verify her identity. This scam can appear even more real when the con artist uses a caller ID "spoofing" product which allows the con to display the name and number of the courthouse on the caller ID box.

As with other scams, the internet is making caller ID "spoofing" even easier. There are now websites that offer subscribers, for a nominal fee, a simple web interface to caller ID "spoofing" systems that let them appear to be calling from any number they choose. Some of these web services boast that they do not maintain logs, and fail to provide any contact information. Some even offer voice scrambling services, which make the caller sound like someone of the opposite sex.

Callers do not necessarily need to utilize a "spoofing" website to manipulate caller ID information. Some providers of Voice over Internet Protocol, or VoIP, services allow their customers to tinker with the caller ID information. Certainly this may not always be done for a deceptive or malicious purpose, but it offers those who wish to do harm an easier way to part consumers with their money.

I understand that the FCC is currently investigating the caller ID "spoofing" problem, but I find it hard to believe that today, there is no prohibition against sending false or deceptive caller ID information. H.R. 5126, the Truth in Caller ID Act of 2006, would remedy that problem in short order.

H.R. 5126 specifically prohibits sending misleading or inaccurate caller ID information. It covers traditional telephone service, as well as VoIP calls, and provides a specific exemption for authorized law enforcement actions. I understand that there may be a need for additional exemptions, and I am anxious to hear from our witnesses how the exemption issue should be handled as we move toward a markup.

Consumers use caller ID services to protect themselves from unwanted calls and contact, including from those who may want to do them harm. They should be able to rely on the caller ID information coming to them on a caller ID box, and H.R. 5126 will do just that.

I was one of the Congressmen that, in the mid-'90s, made sure that caller ID was legal. There were members of this Committee who did not wish to make caller ID a legal service. Thankfully, the majority of the committee, then and now, supports caller ID. I think the majority of this committee, with Mr. Engel's leadership, is going to make sure that we make caller ID exactly what we intended--that is a truthful identifier of who it is that is calling your phone number.

Thank you, Chairman Upton, for holding this hearing today, and I yield back the balance of my time.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you for calling this hearing today on H.R. 5126, the "Truth in Caller ID Act of 2006," introduced by myself and Rep. Engel. This bill is necessary to shut down the growing problem of manipulating caller ID information. Caller ID "spoofing" occurs when a caller masquerades as someone else by falsifying the number that appears on the recipient's caller ID display.

Everyone is familiar with the caller ID product that provides to a consumer the name and number of who is placing an incoming call. Unfortunately, caller ID spoofing is yet another tool available to criminals to hijack the identity of consumers. For instance, the AARP recently ran a "scam alert" when someone posing to be a courthouse employee called a Sterling, Michigan woman claiming that she had missed jury duty that week. The caller threatened that a warrant was being issued for her arrest and then asked her to confirm her Social Security number, to verify her identity. This scam can appear even more real when the con artist uses a caller ID "spoofing" product which allows the con to display the name and number of the courthouse on the caller ID box.

As with other scams, the Internet is making Caller ID spoofing even easier. There are now websites that offer subscribers, for a nominal fee, a simple web interface to caller ID spoofing systems that lets them appear to be calling from any number they choose. Some of these web services boast that they do not maintain logs and fail to provide any contact information. Some even offer voice scrambling services which make the caller sound like someone of the opposite sex.

But a con artist does not necessarily need to utilize a spoofing website to manipulate caller ID information. Some providers of voice over Internet-Protocol, or VoIP, services allow their customers to tinker with the caller ID information. Certainly, this may not always be done for a deceptive or malicious purpose, but it offers those who wish to do harm an easier way to part consumers with their money.

I understand the FCC is currently investigating the caller ID spoofing problem, but frankly, I find it hard to believe that today, there is no prohibition against sending false or deceptive caller ID information. H.R. 5126, the "Truth in Caller ID Act of 2006" remedies this problem.

H.R. 5126 specifically prohibits sending misleading or inaccurate caller ID information. It covers traditional telephone calls as well as VoIP calls, and provides a specific exemption for authorized law enforcement actions. I understand that there may be a need for additional exemptions, and I'm anxious to hear from our witnesses how the exemption issue should be handled as we move toward markup.

Consumers use caller ID services to protect themselves from unwanted calls and contact, including from those who may want to do them harm. They should be able to rely on the caller ID information coming to them on a caller ID box, and H.R. 5126 will do just that.

I want to thank the Chairman Upton for holding this hearing today and I yield back my time.

MR. UPTON. All right. I thank my Chairman, not only for a statement, but also for moving the caller ID legislation a number of years ago. There is nothing, and particularly at dinnertime when somebody

calls, to know exactly who it is, so that we as consumers know whether we should take that call or whether we are going to have cold food for dinner. It is very important. But with that, your statements are made part of the record, and we would like you to try and keep your remarks to not more than five minutes, at which point, when you are completed--all four of you--we will do questions. Again, thank you for your travel to get here promptly on time. Mr. Navin, we will start with you.

**STATEMENTS OF TOM NAVIN, WIRELINE BUREAU CHIEF, FEDERAL COMMUNICATIONS COMMISSION; STACI PIES, VICE PRESIDENT, POINT ONE COMMUNICATIONS, ON BEHALF OF VOICE ON THE NET (VON) COALITION; LANCE JAMES, CHIEF TECHNOLOGY OFFICER, SECURE SCIENCE CORPORATION; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER**

MR. NAVIN. Good morning, Chairman Upton and members of the subcommittee. Thank you for the opportunity to speak about the problem of caller identification, or caller ID, "spoofing".

As we have heard, caller ID services let customers identify who is calling them 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 the telephone call is manipulated in a way 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 about the impact of those practices on the public trust and confidence in the telecommunications industry. We also are particularly concerned about how this practice may affect the public safety and law enforcement communities.

The Commission addressed caller ID on the Public Switched Telephone Network, or PSTN, in 1995, with Commission Rule 64.1601, which generally requires all carriers using the Signaling System 7, or SS7 protocol, 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.

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 PTSN, via SS7, with harmful real-life consequences in such areas as public safety. For example, as we have heard this morning, the Newark Star

Ledger reported that police in New Brunswick, New Jersey, shut down one city neighborhood for hours, evacuating buildings and closing streets, as a SWAT team surrounded an apartment house. Police had received a call from a girl saying she had been handcuffed and raped in an apartment when the call was, in fact, a hoax. This massive police deployment occurred because the caller ID had been "spoofed" to make the call appear to come from the apartment. Hoaxes like these divert our local public safety resources away from where they are so desperately needed, responding to real emergencies and real threats to our homeland security.

I note that the Committee is considering imposing restrictions on Voice over Internet Protocol, or VoIP providers, that facilitate hoaxes and other harmful practices through caller ID "spoofing". As you know, there are many varieties of VoIP, and the definition of VoIP in this bill, as well as other proposed legislation, could be interpreted to exclude many of them from the reach of the FCC. As the House of Representatives considers legislation affecting VoIP, it should be aware that a restrictive definition of VoIP here, or in other legislation, might establish a statutory precedent that would restrict the Commission's authority to assist public safety and law enforcement in other contexts.

At present, my colleagues in the Commission's enforcement bureau are actively pursuing the issue of caller ID "spoofing". They have issued letters of inquiry or subpoenas to several entities who are apparently engaged in marketing and selling caller ID "spoofing" services to customers. The enforcement bureau continues to gather and analyze information about these companies' practices, their networks, their businesses, and their customers, and other germane information, as well as to analyze enforcement options, some of which may be limited to entities that are not regulated by the Commission. In addition, the enforcement bureau has met with carriers, assembled internal technical experts to address the problem, and begun coordinating with the Federal Trade Commission regarding its efforts to address this problem.

In conclusion, the intentional manipulation of caller ID information, especially for the purposes of fraud or deception, is a troubling development in the telecommunications industry. As Chief of the Wireline Competition Bureau at the FCC, I share your concern about this practice. I look forward to working with this Committee, other members of Congress, Chairman Barton, and the Commission, to ensure the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to speak here today.

[The prepared statement of Thomas J. Navin follows:]

PREPARED STATEMENT OF THOMAS J. NAVIN, WIRELINE BUREAU CHIEF, FEDERAL COMMUNICATIONS COMMISSION

Good morning Chairman Upton, Ranking Member Markey and members of the Subcommittee. Thank you for the opportunity to speak about the problem of caller identification or "caller ID" spoofing.

As you know, caller ID services let customers identify who is calling them 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 way 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 concerned about how this practice may affect the public safety and law enforcement communities in particular.

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 FCC 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. Among other things, SS7 conveys information 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. In one particularly harmful way, caller ID spoofing threatens our public safety. Spoofers can fabricate emergency calls and cause local law enforcement and public safety agencies to deploy their resources needlessly. The Newark Star-Ledger reported that police in New Brunswick, New Jersey shut down one city neighborhood for hours, evacuating buildings and closing streets as a SWAT team surrounded an apartment house. Police had received a call from a girl saying she had been handcuffed and raped in the apartment, when the call was a hoax. Caller ID had been spoofed to make the call appear to come from the apartment. Hoaxes like these divert our local public safety resources away from where they are so desperately needed – responding to real emergencies and real threats to our homeland security.

My colleagues in the Commission's Enforcement Bureau are actively pursuing the issue of caller ID spoofing. They have issued letters of inquiry or subpoenas to several entities who are apparently engaged in marketing and selling caller ID spoofing services to customers. The Enforcement Bureau continues to gather and analyze information about these companies' practices, their networks, their businesses, their customers, and other germane information, as well as analyze enforcement options, some of which may be limited as to entities that are not regulated by the Commission.

In addition, the Enforcement Bureau has met with carriers, assembled internal technical experts to address the problem, and begun coordinating with the Federal Trade Commission regarding its efforts to address this problem.

Finally, I note that the Committee is considering imposing restrictions on voice over Internet protocol, or VoIP providers that facilitate caller ID spoofing. As you know, there are many varieties of VoIP, and the definition of VoIP in this bill, as well as other proposed legislation, could be interpreted to exclude many of them from the reach of the Commission. As the House of Representatives considers legislation affecting VoIP, it should be aware that a restrictive definition of VoIP here or in other legislation might establish a statutory precedent that would restrict the Commission's authority to protect life and property in both the public safety and law enforcement contexts.

In conclusion, the intentional manipulation of caller ID information, especially for the purposes of fraud or deception, is a troubling development in the telecommunications industry. As chief of the Wireline Competition Bureau at the FCC, I share your concern about this practice. I look forward to working with this Committee, other Members of Congress, Chairman Martin and the Commission to ensure the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to speak with you today.

MR. UPTON. Thank you. Ms. Pies?

MS. PIES. Thank you, Chairman Upton, Ranking Member Markey, and members of the subcommittee. My name is Staci Pies. I am Vice President of Governmental and Regulatory Affairs for PointOne, a VoIP provider, and President of the Voice on the Net Coalition, the VON Coalition, which is the voice of the VoIP industry. On behalf of the VON Coalition, I thank the Subcommittee for this opportunity to testify about this important issue.

Before I address caller ID in particular, I would like to commend Chairman Barton for his leadership in the committee and subcommittee for taking action in the recent COPE bill to accelerate the availability of VoIP, and the ability to deliver E911 information along with 911 calls. Particularly with respect to members, the creation of a national emergency routing number administration will assure that VoIP providers can obtain necessary pseudo-numbers in a timely fashion.

VoIP providers who have made real strides in leveraging the power of caller ID to provide innovative services to consumers support this committee's effort to protect the integrity of caller ID functionality. We fully agree that 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, as mentioned by Mr. Engel. Congress is right to focus its intention on those who would do so.

VoIP is burgeoning in popularity with consumers and businesses because it can do what plain old telephone service does, but often much, much more. 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. With VoIP, I can direct certain calls to my work phone and others to my home or mobile

phone. I can screen calls and designate some calls at specific times of day, for instance, during the family dinner hour, to be sent straight to voice mail. Some VoIP services even flash caller ID information on the TV screen, making it an easier decision to ignore the call in favor of C-SPAN. VoIP providers allow consumers to integrate technologies in innovative ways, to bring the power and potential of the Internet to voice communications.

Many of the great benefits of VoIP to consumers and business users depend on accurate and non-misleading identification of the calling party. Businesses that use caller ID to call up a customer's account record so that it is immediately available to the customer service representative will not find the record very useful if it is the wrong record because the caller ID has been "spoofed". At the same time, VoIP often allows users greater control over their personal privacy by allowing them to block the caller ID with a click of a mouse.

As Congress addresses deceptive "spoofing," though, we urge you to keep in mind that in some legitimate instances, it can be necessary or desirable to change caller ID information where the purpose is not to mislead or deceive, or where the modification is necessary for a public purpose. 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 would like to share five examples:

As referenced by Mr. Terry, the FCC has created specific rules regarding what kind of caller ID information telemarketers should send, in order to empower consumers to take steps to protect their privacy. Barring any change to calling ID information would prohibit compliance with this FCC rule.

Second, one of the benefits of VoIP is that it can help a consumer better protect her own privacy and manage which of her personal information she presents to the world, irrespective of which communications device she picks up to initiate a call. Calls for different purposes, personal versus business, may merit different telephonic return addresses, as one might do with ordinary mail. This is not meant, however, to sanction masquerading as another.

Third, there are also situations in which caller ID information can endanger individual safety. Of course, as mentioned this morning, the classic situation is battered spouse. In some instances, blocking the delivery of caller ID information might be sufficient, but any legislation should be careful about presuming that blocking will always be adequate.

A fourth example is that in some circumstances, such as with forwarded calls, caller ID information needs to be altered to ensure that

the original calling party's number is transmitted as the caller ID information rather than an intermediate number.

And, finally, as I referenced at the beginning of my remarks, for E911 systems, pseudo-numbers need to be inserted and used, as this Committee has recognized in the COPE bill.

I would like to close with three additional thoughts. First, that "spoofing" of caller ID is not new. Tools have been widely available for years to "spoof" caller ID on traditional networks. As Tom mentioned, the Commission has already addressed these issues. One website even allows the ability to download "spoofing" software from the Internet, and then you can just use a common tape recorder to "spoof" the caller ID.

Second, fighting misleading and deceptive changes in caller ID is only part of the solution. Companies handling sensitive information must also make sure they are handling that information with care.

And third, misleading people through the misuse of caller ID, whether for a prank, or 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 or VoIP service providers who merely transmit what may turn out to be altered caller ID information. When good technology is used for bad purposes, we would like to make sure that it is the bad use of the technology, not the unknowing technology itself which carries the burden.

In focusing on those few people who would abuse caller ID technology, Congress can address the very real problem of "spoofing" effectively, in a cost-efficient manner that protects the proper use of this technology. Together, with this committee's previous efforts to enable consumers to take advantage of VoIP benefits, we believe VoIP is in position to help make communicating 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 I can.

[The prepared statement of Staci Pies follows:]

PREPARED STATEMENT OF STACI PIES, VICE PRESIDENT, POINTONE COMMUNICATIONS, ON BEHALF OF VOICE OF THE NET (VON) COALITION

Thank you, Chairman Upton, Ranking Member Markey, 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.

Before I address caller ID in particular, I would like to commend the Committee and Subcommittee for taking action in the recent COPE bill to accelerate the ability of VoIP to deliver E911 information along with 911 calls. Those provisions, along with what I hope will be a liability provision that can be adopted when the bill comes before the full

House, help ensure that VoIP providers can accelerate E911 solutions through access to the necessary facilities, databases and numbers required to deliver E911. Particularly with respect to numbers, the creation of a national emergency routing number administrator will ensure that VoIP providers can obtain necessary pseudo-ANI numbers in a timely fashion. Leaders from this committee have written to the FCC suggesting they create such an administrator, and so have standards groups, but to date the FCC has unfortunately not done so. That makes it important that this committee adopt E911 legislation this year.

VoIP is burgeoning in popularity with consumers because it can do what Plain Old Telephone Service does – and often much much more. 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. With VoIP, I can direct certain calls to my work phone, and others to my home or mobile phone. I can specify in what order I want my devices to be rung. I can screen calls and designate some calls at specific times of the day (for instance, during the family dinner hour) to be sent straight to voice mail. Some VoIP services even flash caller ID information on the TV screen, making it an easy decision to ignore the call in favor of . . . CSPAN. VoIP allows consumers to integrate technologies in innovative ways – it allows them to integrate voice mail, text messages, and voice services; to bring the power and potential of the Internet to voice communications.

These Internet based voice advances are giving consumers new choices, better prices, and advanced new features.

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 usefulness of their services, VoIP providers have a strong interest in having Caller ID be accurate and non-misleading. At the same time, VoIP often also allows users greater control over their personal privacy by allowing them to block their caller-ID with the click of a mouse.

Moreover, we fully agree that 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. Media reports about spoofers calling police and drawing out SWAT teams are inexcusable and potentially life threatening. A stalker spoofing Caller ID to harass victims, or identity thieves pretending to be their victims are things every American should care about. Spoofing to deceive, defraud, or harass 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, though, we urge you to keep in mind that in some legitimate instances it can be necessary or desirable to change caller ID information – where the purpose is not to mislead or deceive, or where the modification is necessary for a public purpose. 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, the FCC has created specific rules regarding what kind of caller ID information telemarketers should send. Telemarketers are required to transmit as caller ID a number to which a consumer can make a do-not-call request, rather than the telephone number from which the call is placed. The FCC did so deliberately in order to empower consumers to take steps to protect their

privacy. Barring any change to caller ID information could prohibit compliance with this FCC rule.

- Second, one of the benefits of VoIP is that it can help a consumer better protect her own privacy and manage which of her personal information she presents to the world, irrespective of which communications device she picks up 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. This is not meant, however, to sanction masquerading as another.
- Third, there are also 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. But any legislation should be careful about presuming that blocking will always be adequate.
- A fourth example is that, in some circumstances, such as with forwarded calls, caller ID information needs to be altered to ensure that the original calling party's telephone number is transmitted as caller ID, rather than an intermediate number.
- And finally, as I mentioned at the beginning of my remarks, for E911 systems pseudo ANIs need to be inserted and used as this committee has recognized in the COPE bill.

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 website offers the ability to download spoofing software from the Internet which then allows a common tape recorder to spoof caller ID.

Second, fighting misleading 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.

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 altered caller ID information When good technology is used for bad purposes we'd like to make sure it's the bad use of the technology, not the unknowing technology itself, which carries the burden. 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 spoofing effectively, in a cost-efficient manner that protects the proper use of this technology. VoIP service providers, who have made real strides in leveraging the power of Caller ID to provide innovative services to consumers, fully support this Committee's efforts to protect the integrity of caller ID functionality. Together with this committee's previous efforts to enable consumers to take advantage of VoIP benefits, we believe VoIP is positioned to help make communicating 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 I can.

MR. UPTON. Thank you. Mr. James?

MR. JAMES. Good morning.

MR. UPTON. That button.

MR. JAMES. Good morning, Mr. Chairman, Mr. Engel, and other members of the committee. I want to thank you for giving me the opportunity to speak on this topic today, a very important issue.

As one of the founders of Secure Science Corporation, an Internet security and research company, I personally witness the extent to which the abuse and misuse of Caller ID can have. In August of 2004, our investigation team discovered that two of the Nation's largest telecommunications providers, T-Mobil and Verizon, were vulnerable to a technique known as caller ID "spoofing". This technique is entirely reliant upon the manipulation of caller ID to be successful and enables the attacker's access to individual customer's voicemails without using a PIN code, violating both customer privacy and authentication protocols to cellular and land-line voicemail networks.

Similar intrusions, also known as exploits, include unauthorized termination of customer accounts, anonymous automatic phone SPAM, and the potential to gain full administrative control over a major telecommunications network that serves both businesses and residential phone lines. This last possibility is one of the greatest concerns in conjunction with the inappropriate and unlawful uses of caller ID and could even be viewed as a threat to national security in much the same way as the destabilization of a utilities plant or traffic control station could be.

Other exploits employing caller ID "spoofing" have been used by criminals who con unsuspecting victims out of money and in many cases their identity. These individuals are titled as phishers and the activity is phishing, spelled with a p-h. This activity involves the utilization of information gained illegally by breaking into a potential victim's voice mail account. This in turn allows the phishers to further victimize customers by using, for example, billing information to steal identities and garner even more personal information from other sources. Conversely, phishers will use caller ID "spoofing" in order to pose as a victim's bank and phish the account via phone. This same method is also used to lure wire transfer delivery services, such as Western Union, into authorizing fraudulent transfers over the phone. Additionally, phishers will verify their access to the stolen accounts by using the victim's contact numbers in an attempt to validate account availability and amounts by calling the banks themselves and "spoofing" the caller ID as the user of the account.

Because of the level and quantity of illegal activities participated in by phishers, anonymity is one of their primary objectives. Caller ID

"spoofing" enables them not only to communicate covertly with one another, but also provides them with an advantage against law enforcement agencies. As a direct result, the phishers continue their operations all the while evading subpoena attempts.

The aforementioned instances are just some of the many ways in which the fraudulent uses of caller ID are being employed today. Our company's research alone demonstrates that more than 75 percent of the transactions and/or "spoofed" calls made on providers' networks were with mal-intent. This was actually conducted by--we work a lot with Anti-Fraud, with covert calling web services out there--companies that do caller ID "spoofing". And we basically help them try to eliminate the fraud. But we are seeing about 75 percent of the activity is actually fraudulent.

Despite the dark side of caller ID "spoofing," there are very tangible benefits associated with this technique when used in a responsible manner. Secure Science Corporation is often called upon to assist companies who provided automated caller ID "spoofing" service to detect and prevent fraudulent activity on their network. And in order to do this successfully, it is not unusual for us to aid law enforcement by using caller ID "spoofing" techniques to track down these perpetrators. By accessing the very information they attempt to conceal, phishers and other criminals are not successful in their evasive actions, thus increasing the amount of successful investigations with law enforcement involvement brought forth against them. We use a technique that actually allows us to track down the phone numbers they are using. And we have to use a caller ID manipulation technique to do these type of techniques, so there are some very legitimate applications, especially in law enforcement.

One of the most common reasons for the manipulation of caller ID information is executed by the vast majority of Voice over IP companies, as well as those businesses which use private branch exchanges, better known as PBXs. In this case they appropriately utilize the technique so as to provide their telephone communications user with a viable and fiscally prudent alternative to traditional long distance services. One such legitimate caller ID "spoofing" is the transmission of the caller's home telephone number on a Voice over IP call.

With respect to the positive and welcomed uses affiliated with caller ID "spoofing" such as research, investigative tactics, and public services, it is my recommendation as a representative of the information security community that the exemption to this bill be either expanded to include the above mentioned uses, or that the term "illicit" be added to the general wording of the bill. This way, the legitimate academic and

commercial entities and the law enforcement agencies they aid, will not unduly suffer the effects of this proposed Act.

The implementation of the Truth in Caller ID Act of 2006 will without a doubt prove to be instrumental in the fight against the criminal activities in, and the abuse of, our Nation's telephone communication systems. By recognizing this bill as an amendment to the Communications Act of 1934, our government will continue to send the message of intolerance towards those who seek to take advantage of burgeoning technologies for illegal and/or unethical use.

Thank you very much.

[The prepared statement of Lance James follows:]

PREPARED STATEMENT OF LANCE JAMES, CHIEF TECHNOLOGY OFFICER, SECURE SCIENCE CORPORATION

The "Truth in Caller ID Act of 2006" is being introduced with the goal of preventing criminal activities and/or the obstruction of justice with respect to the manipulation of caller identification information.

As one of the founders of Secure Science Corporation, an Internet security and research company, I have personally witnessed the extent to which the abuse and misuse of caller ID can have. In August of 2004, our investigation team discovered that two of the Nation's largest telecommunications providers (T-mobile, Verizon) were vulnerable to a technique known as "Caller-ID Spoofing". This technique is entirely reliant upon the manipulation of Caller ID to be successful and enables the attacker access to individual customer's voicemail without using a PIN code, violating both customer privacy and authentication protocols to cellular and land-line voice mail networks. Similar intrusions, also known as "exploits", include unauthorized termination of customer accounts, anonymous automatic phone SPAM, and the potential to gain full administrative control over a major telecommunications network that serves both business and residential phone lines. This last possibility is one of the greatest concerns in conjunction with the inappropriate and unlawful uses of caller ID and could even be viewed as a threat to national security in much the same way as the destabilization of a utilities plant or traffic control station would be.

Other exploits employing Caller ID Spoofing have been used by criminals who con unsuspecting victims out of money and in many cases their identity (also called "Phishers" and their methods "Phishing"). This activity involves the utilization of information gained illegally by breaking into a potential victim's voice mail account. This in turn allows the phishers to further victimize customers by using, for example, billing information to steal identities and garner even more personal information from other sources. Conversely, Phishers will use Caller ID Spoofing in order to pose as a victim's bank and phish the account via phone. This same method is also used to lure wire transfer delivery services (such as Western Union) into authorizing fraudulent transfers over the phone. Additionally, Phishers will verify their access to the stolen accounts by using the victim's contact numbers in an attempt to validate account availability and amounts.

Because of the level and quantity of illegal activities participated in by Phishers, anonymity is one of their primary objectives. Caller ID Spoofing enables them to not only communicate covertly with one another, but also provides them with an advantage against law enforcement agencies. As a direct result, the Phishers continue their operations all the while evading subpoena attempts.

The aforementioned instances are just some of the many ways in which the fraudulent uses of Caller ID are being employed today. Our company's research alone demonstrates that more than 75% of the transactions and/or spoofed calls made on providers' networks were with mal-intent.

Despite the dark side of Caller ID Spoofing, there are very tangible benefits associated with this technique when used in a responsible manner. Secure Science Corporation is often called upon to assist companies who provide automated Caller ID Spoofing services to detect and prevent fraudulent activity on their network. In order to do this successfully, it is not unusual for us to aid law enforcement by using Caller-ID Spoofing techniques to track down these perpetrators. By accessing the very information they attempt to conceal, Phishers and other such criminals are not successful in their evasive actions, thus increasing the amount of successful investigations with law enforcement involvement brought forth against them.

One of the most common reasons for the manipulation of Caller ID information is executed by the vast majority of Voice-Over-IP companies, as well as those businesses which use Private Branch Exchanges, better known as PBX's. In this case they appropriately utilize the technique so as to provide their telephone communications users with a viable and fiscally prudent alternative to traditional long distance services. One such legitimate use of Caller ID Spoofing is the transmission of the caller's home telephone number on a Voice-over-IP call".

With respect to the positive and welcomed uses affiliated with "Caller ID Spoofing" such as research, investigative tactics, and public services, it is my recommendation as a representative of the information security community that the exemption to this Bill be either expanded to include the above mentioned uses, or that the term "illicit" be added to the general wording of the Bill. This way, the legitimate academic and commercial entities (and the law enforcement agencies they aid) will not unduly suffer the effects of this proposed Act.

The implementation of "The Truth in Caller ID Act of 2006" will without a doubt prove to be instrumental in the fight against the criminal activities in, and the abuse of, our nation's telephone communication systems. By recognizing this Bill as an amendment to the "Communications Act of 1934", our government will continue to send the message of intolerance towards those who seek to take advantage of burgeoning technologies for illegal and/or unethical use.

Lance James
Chief Technology Officer
Secure Science Corporation

MR. UPTON. Five seconds to spare. You did very well. Mr. Rotenberg?

MR. ROTENBERG. Thank you very much, Chairman Upton, Mr. Engel, members of the subcommittee. My name is Marc Rotenberg. I am Director of the Electronic Privacy Information Center. We focus on emerging privacy issues. We appreciate the opportunity to be before the subcommittee again and to testify on the Truth in Caller ID Act, H.R. 5126.

From our perspective, there are two different privacy interests at issue here. The first, of course, concerns the privacy interest of the person's telephone number who would be disclosed to the call recipient. And there are many legitimate circumstances under which a person

would rightfully not want to have their telephone number disclosed. Both Ms. Pies and Mr. James have described instances in their industry and their research where they would also see customers who would not provide their own telephone number or would, for legitimate business purposes, provide someone else's telephone number. But of course, there are also circumstances under which providing a number that is not your own can lead to fraudulent activity, can place public safety at risk. And so we certainly understand the intent of the bill's sponsors to ensure that misrepresenting a person's telephone number does not enable any type of conduct that is criminal or puts the public at risk.

This debate is very similar, in fact, to the debate that took place when the caller ID service was originally offered. And as you may recall at that time, Congress worked with the FCC and the State public utility commissions to establish some privacy safeguards, such as per call blocking or per line blocking, to ensure that people who have a legitimate reason to withhold the disclosure of their telephone number would be protected.

So our view regarding this legislation is that it is appropriate to protect both privacy interests. And the way to do that would be to distinguish between the legitimate and illegitimate types of "spoofing" that might occur. And I think the simple way that you could accomplish this goal would be to add an intent requirement, so that you would make the illegitimate "spoofing" of a telephone number, that which occurs with the intent to defraud or harass the call recipient. I think that would cover virtually all of the circumstances that have been described so far and at the same time ensure that the legitimate uses by businesses and by residential telephone customers would be protected.

I also indicate in the testimony that particularly with the introduction of new Internet-based telephone services, such as Voice over IP, where people will be providing different types of information in the network environment, I think there are actually some First Amendment issues where people who might be broadcasting information over Voice over IP service would have the right to withhold their identity. And I think that is an interest that the Supreme Court has recognized and certainly one that Congress would not want to prohibit people from acting upon.

So I think in addition to protecting the privacy of telephone customers, there are also important free speech reasons why people should not be required to dispose their personal telephone numbers, unless they intend to cause harm, to engage in fraud, or to harass. There are, as you know, Mr. Chairman, statutes that are also available to punish those types of activities when hey occur.

Finally if I may, I wanted to say just a brief word about our filing yesterday at the FCC regarding the recent disclosure concerning the

possibility that the National Security Agency may have established a large database on call detail information. I understand that this issue is a little bit outside the purview of the Subcommittee, but at the same time it is very much related to this issue about the privacy of telephone numbers. We have asked the Chairman of the FCC, Mr. Martin, to open an investigation into the question of whether Section 222, which was the provision of the Communications Act that requires telephone companies to protect the privacy of the call record information that they have obtained has been violated. We very much hope that the members of the Subcommittee will support that effort. We know that Mr. Markey has already indicated that he believes that the FCC should undertake an investigation in this matter, and Commissioner Michael Cobbs has expressed support for that as well.

Anyway, these are the main points of my testimony. As I said, I think it is important to distinguish between the legitimate and illegitimate circumstances where caller ID "spoofing" might occur. And I would be pleased to answer your questions.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Chairman Upton, Ranking Member Markey, and members of the subcommittee, thank you for the opportunity to testify today on caller ID spoofing and H.R. 5126, the Truth in Caller ID Act of 2006. My name is Marc Rotenberg and I am President and Executive Director of 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 a caller not to have his or her identity broadcast with every phone call made. There are many circumstances where it is not necessary for a person's phone number to be disclosed. In fact, in some cases, a person's safety may be placed at risk. 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 bill 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 cause harm. By adding a requirement that an offender act "with the intent to defraud or harass" the call recipient, we believe that H.R. 5126 may provide a tool to protect the privacy of both callers and call recipients. We also have concerns about the provision 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.

The state public utility commissions, the FCC, and the Congress all worked to establish safeguards so that individuals would have some ability to limit the disclosure of their telephone numbers either by means of per-call blocking or per-line blocking. As a general matter, privacy advocates favored per-line blocking for all residential telephone customers because we did not see the benefit in requiring individuals to disclose their phone numbers and we objected to the cost that customers were asked to pay to obtain per-line blocking services.

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.[1]

Anonymous speech is a central facet of the free speech guaranteed by the First Amendment. Without it, speakers with minority opinions are subject to the tyranny of the majority. The Supreme Court has recognized the importance of protecting anonymous speech in a series of cases, including *Watchtower Bible & Tract Society v. Village of Stratton*,[2] *McIntyre v. Ohio Elections Commission*,[3] and *Talley v. California*.[4] In each of these cases, the Supreme Court recognized that, to protect speech, anonymous speech needed to be protected. A speaker's decision to remain anonymous, the Court said in *McIntyre*, "like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[5]

**Caller ID Blocking Does Not Adequately Protect Privacy Interests**

In order to protect telephone users' right to speak anonymously in the face of caller ID, caller ID blocking services were offered. By going through the extra step of dialing *67 before making a call, or by paying for permanent blocking, a user can prevent his or her number from being disclosed to the call recipient.

Despite some of the drawbacks to this system (having to pay for permanent privacy, for instance), 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.

Another problem with requiring callers to disclose the number they call from is that many individuals to protect the have legitimate reasons to report a different number than the one presented on caller ID. For example, a person may well wish to keep her direct

---

[1] *ACLU v. Reno*, 521 U.S. 844 (1997).
[2] 536 U.S. 150 (2002).
[3] 514 U.S. 334 (1995).
[4] 362 U.S. 60 (1960).
[5] *McIntyre*, 536 U.S. at 342.

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.

**Spoofing Can Create Privacy Risks**

This is not to say that caller ID spoofing is an unqualified good--far from it. Earlier this year, EPIC brought to Congress's attention the problem of pretexting consumers' phone records.[6] Pretexting is a technique by which a bad actor can obtain an individual's personal information by impersonating a trusted entity. For instance, pretexters would obtain individuals' phone records by calling phone companies and pretending to be the individuals themselves. This tactic of fraud can be used in other situations as well, such as obtaining an individual's Social Security number by pretending to be the individual's bank or insurance company.

Understandably, caller ID spoofing is an important weapon in a pretexter's arsenal. 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]

Nor can we 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.[8]

**Intent Requirement**

Just as we cannot assume that all those who draw their curtains have something to hide, we cannot assume that every caller who spoofs their number is a bad actor. Callers from within a company might want to keep their direct lines private. Law enforcement informants and whistleblowers who call a toll-free tip line have good reason for keeping their calling information private.

What distinguishes these legitimate uses of spoofing from a pretexter pretending to be a bank in order to get account information, or a cyberstalker spoofing in order to harass his victim, is the intent behind the spoofing. However, as it currently stands, H.R. 5126 does not draw a distinction between these intents.

We believe that the insertion of a phrase--"with the intent to defraud or harass"--into Section 2(e)(1) of the bill will preserve the privacy rights of callers while outlawing fraud and harassment assisted by the technology.

---

[6] *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.

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

**Significance of NSA Surveillance Program for Privacy of Call Records**

Mr. Chairman, it is difficult to comment on the legislation before the Subcommittee today without also noting the recent revelation that the National Security Agency may have constructed a massive database of telephone toll records of American consumers.

Yesterday, 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.

Given the very real possibility that the telephone numbers of American consumers may have been improperly disclosed by the telephone companies to the National Security Agency without legal authority there is the obvious consideration that some telephone customers may choose to take advantage of "spoofing" services to protect their privacy against unlawful surveillance.

Clearly, the issues raised by the NSA program include some matters that are not typically considered by this Subcommittee. But we would urge Members to support EPIC's recommendation that the FCC undertake an investigation of the possibly improper disclosure. If the Communications Act was violated, that should be of concern.

And it would seem doubly unfair for the Committee to push forward legislation that would prevent telephone customers from protecting the privacy of their phone numbers at the same time questions have been raised about whether phone records are subject to unlawful searches.

**Conclusion**

Spoofing caller ID numbers can create a real risk to individuals who might be defrauded by bad actors. However, protecting callers' privacy rights, means that any ban on spoofing take into account the intent of the caller. By prohibiting spoofing with an intent to defraud or mislead the call recipient, the Truth in Caller ID Act would be significantly improved. I will be happy to answer any questions you might have at this time.

MR. UPTON. Well, thank you. Thank you again for your travel from the West Coast and Texas as well. I have a couple of questions and we will proceed on our 5 minutes and rotate among Members here. Mr. Navin, a couple questions for you. Has the FCC actually gotten complaints from folks with regard to "spoofing"? And if so, how many? Has it come to your attention?

MR. NAVIN. I have consulted with our Consumer and Governmental Affairs Bureau and they indicate that they have received approximately 20 complaints--20 more formal complaints on this and perhaps five times that number of inquiries with regard to caller ID "spoofing" in general.

MR. UPTON. And you know, when we passed the Do Not Call List a couple years ago now, and of course the FTC is where we call to get on that list. I do not know if you tried with your counterparts at the FTC as it relates to this at all--maybe we should have asked the Chair when she was here the other day about that issue. Do you know if there has been any communication between the FCC and the FTC in terms of complaints that might have gone to them?

MR. NAVIN. I understand that our enforcement bureau has reached out to the folks at the FTC. I do not know the answer to your specific

question about whether they are doing any investigations themselves. But I know that they are fully aware of our activities in terms of the companies that we have contacted and our efforts to gather more information about this problem. But I cannot speak to what the FTC is actually doing.

MR. UPTON. I would think that if this legislation were to become law tomorrow these companies that are offering their services to "spoof" would likely go out of business like that. Would you suspect that that is the case?

MR. NAVIN. I really could not make a prediction on that. I think that to the extent that they are offering this service to mislead or defraud the customer, I think that they very well may be captured by the legislation. As I understand it, there has also been some debate about adding an intent requirement, and that could certainly play a role in the Commission's ability to enforce the legislation. So I could not say for sure that everyone would go out of business.

MR. UPTON. Okay. I really view this as someone coming to your door. I mean, I like caller ID. Got it on my phones, and I know who it is. It is going to be for my son or it is going to be for my daughter. It is going to be for my wife, me, or whoever it is. And it is very much like someone knocks on your door. Often you look out the little window or--figure out who it is that is coming in. And I do not know if the FCC--have you all ever thought about--do you think that you have the actual rule-making ability to do this without legislation or do you really need legislation to try and prevent "spoofing" from occurring?

MR. NAVIN. Certainly one of the challenges for the Commission as communications have migrated to Internet-based platforms has been the nature of the investigative targets. The Commission finds itself calling on companies that have not traditionally been regulated by the Commission because they are not license holders or entities that have been typically or historically regulated by the Commission. So I think that there is some concern. There is always some concern on the part of the Commission relating to its enforcement authority in the Internet context. And I think that the Commission would be particularly concerned about any restrictive definitions in the legislation as it relates to VoIP service providers. I think that a restrictive definition in this context may have unintended consequences for the Commission in other contexts, including the public safety context and the law enforcement context.

MR. UPTON. Thank you. Mr. Engel?

MR. ENGEL. Thank you, Mr. Chairman.

Mr. Navin, do you think the authority needs or are there things we could possibly add that you think would be helpful?

MR. NAVIN. I would repeat my comment about the definition of VoIP service providers in this bill. The definition of VoIP service providers in this bill would seem to limit the Commission's flexibility to expand the definition to include one-way services, for example, or services that are not offered for a fee. I know that the Department of Justice recently filed with the Commission in another docket--in the CALEA docket--its concerns about any definition of VoIP providers that is restrictive because of the substitution that is going on between communication services today.

MR. ENGEL. Thank you. Ms. Pies, I see in your testimony you mentioned you think people would ignore the phone to continue watching C-SPAN. So my question to you is have you been talking to my mother in Florida? Because she is the only one I know who does that.

MS. PIES. Actually, my father watches C-SPAN all the time and calls me and asks why I have not testified yet, so here I am.

MR. ENGEL. Well, when I come home my wife says--she sees me turning on C-SPAN and she says to me after doing this all day, you come home and turn on C-SPAN. You have got to be kidding. But today is my anniversary and I have been married 26 years, so something has been working. I do not know. Sir, thank you.

MR. UPTON. She is watching right now.

MR. ENGEL. That is why, you see? Now where are the C-SPAN cameras?

MS. PIES. That is a nice gift. Congratulations.

MR. ENGEL. Thanks. Seriously, though. I want to commend the VoIP providers. It is an exciting technology. And many thousands of my constituents have started using Cablevision's Optimum Voice Service. But I understand that there is no standard for VoIP providers when it comes to caller ID. So I want to ask you. Do most programs let someone manually enter any caller ID information they want?

MS. PIES. I can't speak for most VoIP services. I do know that a number of residential services that are designed essentially to replace your plain old telephone service only permit the user to have the numbers that are assigned to them. So for instance, if I could select one number or if I can select five, those are my five numbers and I can use any of them. They are my numbers. Some services that again may be unlawful or illegitimate may not stop that, but I do not actually have knowledge of who those providers might be, if that happens at all.

MR. ENGEL. Thank you. Is the VoIP industry working toward a standard for how to handle this so that it would be uniform?

MS. PIES. That is an interesting question. There are a lot of different standards that are used to transmit calls that originate to IP. In many

instances, IP-originated calls do not have a standard telephone number associated with them. And in those instances, there are no standards but international requirements that the provider can use a different code to transmit. And that code is, I believe, 000123456. Because VoIP calls do not have the same tie to geography that plain old telephone calls have, the phone number is in many instances irrelevant. And so rather than retrofitting our networks to add a phone number that has no meaning, providers often do not engage in any change or manipulation at all.

MR. ENGEL. Thank you. Mr. James, if you could see one thing added, removed, or changed in this bill, what would it be?

MR. JAMES. I would honestly focus on the intent behind the bill. And the reason I say this is because if you look at other crimes that exist on the Internet such as SPAM or phishing--the techniques that are used for phishing are very common. An example as layman as possible, I will try to be--you can mirror a website. You can set up a "spoofed" email. You can then send out the mass mailing. If you look at all three of those techniques specifically, all three of those are legal when they are used legitimately. You can mirror a website. There is nothing wrong with that. You can "spoof" your email if you are showing someone a demonstration. People do it all the time when they change their identity on their email from multiple mail accounts. They literally are just changing their email address, but it is going through a different mail server. And on the third one, you can do the same mass mailing with bulk mail campaigns for marketing that have opt-in lists and all these such things. So there are mainly two things that I would focus on.

I agree with Mr. Navin on the VoIP definition needs to be broadened. And the reason why are we have to also look at successors to VoIP in the sense of--smart homes is a good example. Not all of them are two-way. What if you are doing a home alert safety system for your grandmother and you want to just use VoIP to do the intercom system over the Internet and say are you okay? That is a one-way system. So VoIP could still be utilized in that and that is one-way. So I think that we should open that expansion a little bit. I would recommend going to the U.S. Patent Office, looking up if the definitions of VoIP are defined there, and start maybe using those types of techniques there.

Another thing that I would see to expand on the bill possibly is, agreeing with Mr. Rotenberg on the legitimacy and the illegitimacy concepts. The reason why is--one of the things that I think that might want to be added to the clause of illegitimate activity is that teeth need to be added to this bill. And what I mean by that is that technology should be in place in telecom providers to help detect illegitimate activity so that you can actually enforce this. Because caller ID "spoofing" is essentially anonymous in many cases and it becomes very difficult to track down.

MR. ENGEL. If you would just indulge me, Mr. Chairman, I would like to ask Mr. Rotenberg the same question. I know you mentioned it in your testimony. But if you want to add anything, if you could see one thing added, removed, or changed in the bill, what would it be?

MR. ROTENBERG. Mr. Engel, I think adding the intent requirement is the key addition. And what that effectively does would be to distinguish between the people who are "spoofing" with mal intent and the people who are "spoofing" with a legitimate business purpose or privacy interest. I think virtually all of the witnesses have made a similar point, so I hope it is a change that the Subcommittee would make.

MR. ENGEL. All right. Well, thank you. Mr. Navin, do you want to add anything? I know we talked about the FCC but is there anything else that you would want to add about the bill? If you could see one thing added, removed, or changed, what would it be?

MR. NAVIN. I would emphasize that the Commission will take all steps that it can possibly take to implement the legislation however Congress determines to pass it, but I think it is important that the definition of VoIP services in the bill does not necessarily restrict the Commission's authority as it relates to solving this problem as well as other problems that the Commission faces, including 911 and law enforcement. Thank you.

MR. ENGEL. Thank you. Thank you, Mr. Chairman.

MR. UPTON. Mr. Terry?

MR. TERRY. Thank you, Mr. Chairman. I will go back to my opening statement. I guess the specific question as the bill is written now, under this assumption a tele-services company has a contract with XYZ Corporation to do outbound calls trying to get them to subscribe to more credit card services, let us say, for example. And the telemarketing service is located in Omaha, Nebraska. The client is located in New York City and uses the general number for their client as the caller ID number. So the intent is to use a different number, but one of their client. Mr. Navin, and then I will go down the panel, so we have the intent to use a different phone number. Is that conduct "spoofing" under this bill? And then after that, should it be or should it not be "spoofing"?

MR. NAVIN. As I understand it, the focus of the bill is misleading or inaccurate caller ID information. Based upon the Commission's existing rules that the Commission adopted in 2003, in the Do Not Call proceeding, it does not seem to me that the hypothetical that you gave would fall within the definition of inaccurate or misleading information. Indeed, under the Commission's rules, any person or entity that engages in telemarketing must transmit caller ID information. Any person or entity that engages in telemarketing is prohibited from blocking the transmission of caller ID information. The telemarketers may, however,

substitute for the name and phone number used or billed for making the call the name of the seller on behalf of which the telemarketing call is placed and the seller's customer service telephone number. So according to the Commission's existing rules, which I think were designed to get at the issue of inaccurate or misleading information, I do not think that your hypothetical creates a problem.

MR. TERRY. All right. So there is nothing in this bill that would then, in essence, create an issue of trumping your regulatory language?

MR. NAVIN. I do not believe so. Certainly if necessary you could specifically make reference to the Commission's rules and preserve the Commission's existing rules in this regard to ensure that telemarketers are not captured by this legislation.

MR. TERRY. All right. The other three, I will ask it in a different way. And that is just is that a legitimate business practice for a telemarketer to use the caller ID number of their client instead of it having to come up XYZ Telemarketing? I will just let you go down whether that is acceptable or whether that is fraudulent.

MS. PIES. Not only is it acceptable, and as Mr. Navin mentioned, required by the FCC rules, it is an enabling feature of VoIP technology. As you know, it is not just in the telemarketing business, but it allows jobs to be in-sourced to rural areas, to people who may not be able to get out to a call center. They can actually work from home. Rather than their home number showing up, it would be a central phone number that shows up. So it is actually a very important feature. I am not sure that the legislation as it is drafted today actually gets at allowing it. Probably if you went back and included intent language, as we have discussed, that would be very helpful.

MR. JAMES. The answer to this is it is definitely applicable in marketing, whether it is telemarketing or some other. And I will give an example of that. Two days ago, I saw a Bank of America email talking about their partnership with eHealth Insurance. It was sent by a third party but it said it was from Bank of America. But if you go through the mail headers, it is not really sent from Bank of America's system. It is actually sent from their marketing third party vendor. So in a case such as this, yes, there is a very legitimate use, and I think that I am agreeing with virtually everybody as well on this panel that "legitimate" needs to be defined. If you look at the bill today, it technically could surpass because one would argue misleading. Well, we are not misleading. We are calling on behalf of our client, and technically that falls under this bill that says, we are not misleading anything, but I would want to clarify that further along so that we are not even having to go to a hearing about it and debating the issue or going to court on this issue, so that it is more defined.

MR. ROTENBERG. Mr. Terry, I actually disagree with Mr. Navin's assessment about how the language would be interpreted in this bill. He is referring to earlier legislation and rulemaking that was explicitly enabled by that statute for the FCC to develop regulations and to interpret terms. This bill which is before your subcommittee is, first of all, more recent in time. Secondly, it doesn't incorporate the earlier definitions. And third, it creates no rulemaking authority for the FCC to do so. And, at first impression, if a court looks at the language of this statute, this statute prohibits making a call in which misleading or inaccurate caller identification information is provided. I think those words are fairly straightforward. So in the absence of similar authority for the FCC to conduct a rulemaking and interpret those terms, I think it would not provide protection for the type of tele-services you have described. And I think the better approach would, in fact, be to create an explicit intent requirement that would protect businesses that are not engaging in fraudulent or harassing activity.

MR. TERRY. Very good, thank you.

MR. UPTON. Mr. Inslee?

MR. INSLEE. Thank you. Mr. Rotenberg, just briefly on the issue of surveillance. You indicated that it would be a good idea for Members of Congress to weigh in on this. What would you suggest about a strategy in that regard?

MR. ROTENBERG. Well, Mr. Inslee, we would very much appreciate support from the subcommittee members, certainly of both parties, encouraging Chairman Martin to open an investigation as to whether Section 222 was violated. You know that earlier this year, hearings were held on the question of pre-texting, which is the way in which people's personal telephone numbers became available for sale on the Internet, and a lot of good work was done in this committee, and Chairman Martin testified about the importance of protecting the privacy of those records. Very similar issues, but of course on a much larger scope, have arisen now in the context of the domestic surveillance program, and we hope that Chairman Martin will be encouraged to pursue this investigation.

MR. INSLEE. I will join others in doing that. Just so you know, I will be bringing in an amendment--a little bit related issue on the Defense Department Appropriations Bill that will prohibit the expenditure of taxpayer money for electronic surveillance that does not comply with the FISA law. So we will be having a debate on the House floor here in a few weeks.

MR. ROTENBERG. Thank you.

MR. UPTON. Mr. Engel, do you have additional questions?

MR. ENGEL. Well, I have just one kind of light-hearted question. I understand that our computer engineers are working on what is called

Internet-2. I really, to tell you the truth, don't know a lot about it, but I believe it is supposed to be an upgrade, like going from Windows '98 to XP, and I am sure we will be holding hearings on it. My question is to anybody. Do any of you know if Internet-2 will help this situation that we are talking about it today, or possibly make it worse? Mr. James.

MR. JAMES. If I may? I don't think that--Internet-2 is technically a medium for communication. I was kind of thinking about when I was going through this bill about, one of the reasons why I agree with Mr. Navin about expanding is we could get into a predecessor scenario of VoIP working on an IPX protocol instead of the standard internet TCP/IP protocol, and that would basically not be covered by this bill because it specifically says TCP/IP. And I was actually thinking if Internet-2 is one of the examples, what happens there? Is it going to be using the same protocol? Will it be defined in this bill? I don't think that Internet-2 is going to necessarily secure the techniques against caller ID "spoofing", because the problem is at a protocol layer of the actual VoIP--without getting technical, it is basically a session initiation protocol. It is basically this specific protocol, and that is where the weakness lies. It doesn't really matter what it communicates on. If Internet-2 does buy into, like, cryptographic communication per every communication it ever makes, an authentication on every little communication your computer may make, and so it does accountability and auditing trails and all this. There is a very good chance that we could stem it down because of the fact that we could track the activity itself. But, unless it does something like that, which I don't believe it does at this time, it is not going to be much more effective.

MR. ENGEL. Thank you. If we have hearings about it, we should call you back again. Anybody else?

MS. PIES. Mr. Engel, I just wanted to mention that the committee or subcommittee should approach the definition and what it encompasses cautiously. Certainly, Congress should want to ensure that any legislation enables new technology and the new features that are so important for both residential users and businesses rather than stifling the technology. And the concern that the VoIP industry has is not, certainly, any desire to get out of obligations or to ensure the safety and security of our Nation, but it is that we won't be able to continue to make the investments that will bring these transformative technologies to consumers. And so it is not a specific request, but just sort of a word of caution.

MR. ENGEL. Well, thank you. I appreciate that. Thank you, Mr. Chairman.

MR. UPTON. Thank you, again, for your leadership on this issue. Mr. Navin, I have one last question, and that is if we were to add the

clause or intent to defraud as part of this legislation standard to the bill, how would that affect your efforts to enforce the law?

MR. NAVIN. I think that, from the Commission's vantage point, any time you add an intent standard, it puts an additional evidentiary burden on the Commission in its enforcement process, so I think it would make it more difficult to enforce. The Commission would certainly take all steps necessary to enforce the law, but I think it would indeed make it more difficult.

MR. UPTON. And, with that, I will yield to my friend, Mr. Markey--

MR. MARKEY. Thank you.

MR. UPTON. --in the nick of time.

MR. MARKEY. Thank you so much. Mr. Navin, is it? Navin. In your testimony, you note that the Commission addressed caller ID on the public switch telecom network in 1995, with a rule which requires all carriers using Signaling Systems 7 to transmit the calling party number associated with an interstate call to interconnecting carriers. Did the recently granted Verizon forbearance petition remove this requirement for Verizon?

MR. NAVIN. The Verizon forbearance petition sought flexibility from certain common carrier regulations. I don't specifically recall whether they enumerated this regulation in their petition. The Commission did not deny that petition within the statutorily defined period of time and, according to the statute, if the Commission fails to take action, the petition is deemed granted. So I don't know whether they specifically enumerated this regulation in their petition.

MR. MARKEY. So they did not grant forbearance from all of Title II, is that what you are saying?

MR. NAVIN. My recollection is that there were certain obligations that Verizon carved out of its application, and I know, for example, in an ex parte in the beginning of February, they made it plain to the Commission that their petition did not include asking the Commission to remove the Section 254 obligation, which is the universal service obligation. I also know that in one of those ex partes, they restricted the scope of the petition to exclude certain special access services that they are providing today. So I don't know if they specifically excluded--

MR. MARKEY. You don't know.

MR. NAVIN. --this.

MR. MARKEY. Okay. Did they list Section 222, the CPNI section?

MR. NAVIN. In the original petition, they asked for relief from all common carrier regulation. Section 222 is within the body of law under Title II of the Act, so I think it is certainly arguable that they included, or intended to include, this within the scope of the petition to the extent that they were seeking to get out from Title II.

MR. MARKEY. Okay. So many of us are concerned about allegations that carriers circumvented the Section 222 Customer Privacy rules and gave calling data to the NSA. And yet the FCC recently granted Verizon the right to avoid these rules, and many others, when it granted through inaction the Verizon forbearance petition. Mr. Rotenberg, could you comment on that?

MR. ROTENBERG. Well, Mr. Markey, we are honestly concerned if the telephone companies are trying to get out from under the Section 222 obligations, particularly, as you note, in light of the recent allegations. We are not familiar with the Verizon forbearance petition, but I will point out that this provision of the Communications Act traces its routes, actually, to the original passage, back in 1934, when telephone companies were asked to ensure that the privacy of their customers would be protected. So obviously this would be of great concern.

MR. MARKEY. Okay. Mr. Navin, when do you expect to complete the Notice of Proposed Rulemaking on CPNI?

MR. NAVIN. I believe that we have received comments in that proceeding, but we have not yet received reply comments. I think that we would wait until the record closed before we began the process of presenting options to the commissioners. I think that the reply comment period closes either later this month or early in June, so I think that we will begin to brief the commissioners and present options to them some time thereafter.

MR. MARKEY. Okay. And I would ask you just, Mr. Rotenberg, if you could, just tell me--if you could just summarize the one thing you want us to remember about the issue that we are dealing with in the hearing today?

MR. ROTENBERG. Well, Mr. Markey, on the legislation before the committee, we feel very strongly that an intent requirement needs to be added to distinguish between legitimate and illegitimate uses for caller ID "spoofing". And as for the other issue you raised, we very much support the effort to encourage Chairman Martin to conduct an investigation to Section 222 and the allegation that information was improperly disclosed.

MR. MARKEY. Thank you. Well, I have asked the Chairman of the--I have asked Chairman Martin to give us information as to what exactly has taken place in the relationship between the telephone companies and the NSA so that we can have more information to determine whether or not any privacy laws have been violated, or any other laws that have pass by this Committee that may have been violated. So I thank you, Mr. Chairman, for this lively and entertaining--

MR. UPTON. I didn't see a Starbucks cup there.

MR. MARKEY. --and--which probably means I am not really awake, even if I am sitting here, at this point. But I thank you for the hearing, Mr. Chairman.

MR. UPTON. Thank you all for being here. I appreciate your testimony. I would say that it is my understanding that it is likely that we will move to a markup relatively soon on this bill before the full committee, and I appreciate your input and your thoughts, and we look forward to continuing on a bipartisan path. With that, we are adjourned.

[Whereupon, at 10:19 a.m., the subcommittee was adjourned.]

SUBMISSION FOR THE RECORD BY DAVID SLOANE, SR. MANAGING DIRECTOR, GOVERNMENT RELATIONS AND ADVOCACY, AARP

May 22, 2006

The Honorable Fred Upton
Chair, Telecommunications and the Internet Subcommittee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Upton:

AARP appreciates the opportunity to comment on H.R. 5126, the "Truth in Caller ID Act of 2006." This bill prohibits the transmission of misleading or inaccurate caller ID information.

H.R. 5126 addresses an important issue for mid-life and older Americans. Caller ID "spoofing" occurs when software or technology is used to manipulate caller identification information and alter the calling number that appears on a recipient's telephone. As a result, consumers believe they are receiving a call from someone they trust. The telephone number appears to be correct on their caller ID screen, but in fact, the call is from someone else.

Caller ID spoofing not only creates consumer confusion, it provides yet another tool for scam artists to prey on innocent consumers. H.R. 5126 offers a reasonable solution to address this emerging problem.

Some concerns have been raised that the ability to manipulate caller ID information could offer some positive value to the caller and therefore should not be completely prohibited. For victims of domestic violence and other individuals requiring anonymity, for example, the ability to use this technology to protect their identity might be essential. We encourage the Committee to consider all consumer interests in this issue.

Again, we commend the sponsors of H.R. 5126 for raising this important consumer issue. We look forward to working with the members of the Committee in crafting legislation that provides practical protections for all consumers, and especially vulnerable older persons.

Sincerely,

David Sloane
Sr. Managing Director
Government Relations and Advocacy

○