Department of Justice

STATEMENT

OF

BARRY M.SABIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

H.R. 740, A BILL TO AMEND TITLE 18, UNITED STATES CODE, TO PREVENT CALLER ID SPOOFING AND FOR OTHER PURPOSES

PRESENTED ON

FEBRUARY 6, 2007

Statement of Barry Sabin
Deputy Assistant Attorney General
Criminal Division, U.S. Department of Justice
Before the U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Concerning
H.R. 740, A Bill to Amend Title 18, United States Code, to Prevent Caller ID Spoofing and for Other Purposes

I.
Introduction

Good morning, Mr. Chairman, Ranking Member Forbes, and Honorable Members of the Subcommittee. It is my pleasure to appear before you to discuss H.R. 740, the PHONE Act of 2007, a bill to prevent caller ID spoofing. The United States Department of Justice supports Congressional action such as this to give law enforcement better tools to protect our citizens and our country from identity thieves, stalkers, and other criminals.

This bill targets a telephone calling practice known as "caller ID spoofing." Caller ID spoofing is the modification of caller ID information that causes the telephone network to display a number and other information on the recipient's caller ID display that is not the number of the actual caller.

Recently, caller ID spoofing services have become widely available, greatly increasing the number of people who have access to this tool to deceive others. By outlawing the misuse of caller ID spoofing, this bill, with modifications we will recommend today, can improve the Department's ability to prevent crimes ranging from identity theft to harassment to pretexting.

I note that I testified in a hearing on November 15, 2006, concerning a similar bill, H.R. 5304, the "Preventing Harassment through Outbound Number Enforcement Act" ("PHONE Act"), which passed the House in the 109th Congress, on December 9, 2006.

II.
Caller ID Spoofing Is Being Used By Criminals to Commit Crimes Such as Identity Theft and to Invade Americans' Privacy.

Criminals can use caller ID spoofing to facilitate a number of crimes, including identity theft, harassment, privacy invasions, and even election fraud. Obviously, caller ID spoofing can help to hide the identity of a criminal, but it can go farther, actually defeating security measures that would have prevented a crime.

For example, caller ID spoofing can lend credibility to a criminal trying to trick an individual into giving up private information, such as a credit card number or social security number. By making it appear that the call is coming from a legitimate charity or bank, from a business's customer, or even from the office of a political campaign, criminals can more easily fool victims into giving up private information. For instance, a "pretexter" can call telephone companies pretending to be a subscriber and try to obtain the subscriber's private telephone records. If the caller ID information matches the subscriber's home telephone number, the pretexter can more easily gain access to those private records.

Caller ID spoofing can also create opportunities for abusers who could not otherwise contact their victims to reach into those victims' homes and further harass them. Misleading caller identification information could cause a victim to accept a call they would otherwise avoid or circumvent automatic call-blocking that would have prevented the harassing call from being connected.

Identity thieves, hackers, and other criminals might also use caller ID spoofing to circumvent security measures put in place by financial institutions, money transfer agents, communication service providers, retailers, and restaurants. Such businesses sometimes use

caller ID information as part of their fraud prevention measures as a way of confirming the identity of the caller. If the information fed into these systems is inaccurate, the security measures might be defeated and allow transactions or access to private information that would otherwise have not been permitted.

These concerns are not theoretical; we know that criminals are using these caller ID spoofing services to further their crimes today. Take, for instance, the case of James Turner Hopper, who pleaded guilty to several federal felony offenses involving identity theft. Hopper admitted that he obtained over 100 credit card numbers and associated identity information. He then placed calls to a money transfer agent and used the stolen credit card accounts to send money to himself and others. To make these calls, Hopper used a caller ID spoofing service in order to hide his true identity and to defeat internal security controls that would have disclosed that he was using other peoples' credit card numbers. Hopper was able to use this tactic more than 150 times while attempting to steal over $88,000. The United States District Court for the Southern District of California recently sentenced Hopper to 30 months in prison.

In another instance, a criminal used caller-ID spoofing and voice-alteration software to repeatedly call a police officer and threaten to kill the officer and his family. Because the criminal spoofed the caller-ID, it became very difficult to determine the source of the calls.

III.
Caller ID Spoofing Services Have Become Widespread and Readily Available to the Public.

Recent changes in technology have made caller ID spoofing easier and less expensive, which has led to services that allow many who would otherwise lack the necessary technical

sophistication or equipment to spoof caller ID to be able to do so from any telephone or Internet connection.

Widely available Voice-over-Internet-Protocol (VOIP) equipment can be configured to populate the caller ID field with information of the user's choosing. Equipment owners can allow users to connect to their equipment through the Internet or through toll-free telephone numbers. Once connected to the spoofing service, users can place a call to any other telephone and choose what telephone number they wish their recipients to receive. Numerous spoofing services exist today that allow anyone to change his or her caller ID information simply by placing a call through a toll-free number or by setting up the call through the Internet.

It is the widespread availability of these new services that has brought caller ID spoofing to the mainstream. While this development is relatively new, we are already seeing that the capability is being misused to facilitate crimes and could be used to hamper investigations.

Addressing the problem, of course, must be done carefully. We understand that modifications to caller ID information can be done for benign or even beneficial purposes. There are instances where caller ID information is modified to accurately reflect the calling party, such as when companies hire outside telemarketers to call customers. In such cases, the caller-ID information transmitted is that of the actual company, allowing those receiving the call to have a reliable way to call back. No one is misled as to the identity of the calling party.

It has been claimed that caller ID spoofing serves to protect people's privacy. Yet, a caller who wishes to remain anonymous already has an option to use caller ID blocking, preventing his or her number from being known. Simply put, the caller gets to make a choice about whether to reveal his or her number, and the called party gets to make a choice about

whether to accept an anonymous call. By contrast, transmitting information that misleads the called party does not provide any additional privacy benefit.

Some have further suggested that, as an alternative to blocking caller ID information, individuals would benefit from being able to modify caller ID information in order to provide alternative call-back information. While this could in some instances be a non-objectionable use, today, there is no requirement that providers of caller ID spoofing services make any effort to verify that the person requesting to place a call with altered caller ID has any right to use the number requested. This lack of verification provides opportunities for misuse. Moreover, the widespread availability of caller ID spoofing services could complicate criminal investigations. For example, if kidnappers or terrorists were to use caller ID spoofing, law enforcement involved in fast-moving investigations could lose valuable time chasing down the wrong path.

IV.
This Bill Could Be Improved to More Effectively Combat the Harms Caused by Widely Available Caller ID Spoofing.

The Department is concerned with the widespread availability of caller ID spoofing services that present significant potential for abuse and hinder law enforcement's ability to investigate crime. Overall, the bill supports the Department's efforts to combat the threats caused by caller ID spoofing. The Department was pleased to see that the scope of the bill includes both conventional telephone calling and many types of VOIP services.

The Department has a number of other recommendations to clarify and strengthen the bill and to make it more effective.

A. The bill can be made more effective by clarifying and simplifying the description of the offense.

The current version criminalizes the acts of a person who "knowingly uses or provides to another (1) false caller ID information with intent to defraud; or (2) caller ID information pertaining to an actual person without that person's consent and with intent to deceive the recipient of a phone call about the identity of the caller."

First, the statute's reference to "using or providing" is potentially confusing. We suggest substituting the words "modify," "generate," and "transmit." The word "provide" invites confusion between a person "providing" misleading caller ID information and a "provider" of telecommunications or VOIP services. Furthermore, the terms "uses" and "provides" might be thought to apply to carriers who use the misleading information for billing or some other purpose.

Second, requiring proof of fraud in most cases may permit some culpable conduct to escape prosecution. There are categories of crime other than fraud, such as telephone harassment or stalking, that may exploit caller ID spoofing.

Third, the term "actual person" is not defined in the bill and its meaning is unclear because "actual person" may not cover companies or other entities such as government agencies. We believe that caller ID information for companies and other entities is as susceptible as an individual's caller ID information to exploitation for criminal purposes. For example, a criminal could pretend to be calling from a victim's doctor's office in an effort to trick the victim into revealing sensitive information. We recommend deleting the word "actual" from this proposed subsection and adding a definition of the remaining term "person" in subsection (e) The definition should refer to the meaning of "person" given in 18 U.S.C. § 1030, which explicitly includes government entities.

Fourth, because spoofing might be used to fool telephone carriers about the jurisdictional nature of a call, the prohibition should refer to an intent to deceive "any other person," rather than just the recipient of a call.

Fifth, because the definition of the offense appears to require that a telephone call be made before a crime is committed, we recommend that the jurisdictional hook be changed from the more narrow "in or affecting interstate or foreign commerce" to the broader ","using any facility or means of interstate or foreign commerce, i.e., a telephone (pursuant to 18 USC § 2422(b)). Under the former hook an interstate call would be required, while under the later hook any telephone call would suffice.

Thus we recommend changing the language to:

> (a) OFFENSE. -- Whoever, ***using any facility or means of interstate or foreign commerce,*** knowingly ~~uses or provides to another~~ ***modifies, generates, transmits, or causes to be modified, generated, or transmitted—***
>
> > (1) false caller ID information with the intent to ~~defraud~~ ***commit, or to aid or abet any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law;*** or
> > (2) caller ID information pertaining to a person without that person's consent and with intent to deceive ***any other person*** about the identity of the caller;
>
> or attempts or conspires to do so, shall be punished as provided in subsection (b).
>
> (e) DEFINITIONS. —
> ***(6) the term 'person' has the meaning given that term in section 1030 of title 18, United States Code.***

B. The bill could be made more effective by creating a more graduated series of punishments.

The proposed bill establishes only two levels of punishment, a felony for offenses committed "for commercial gain," and a misdemeanor for other offenses. Some of the most shocking uses of caller ID spoofing, however, have not been for commercial gain, such as when

SWAT teams have been summoned to a house in response to a false hostage situation. The drafters may wish to consider expanding the types of offenses that would merit felony prosecution to include, for example, caller ID spoofing done in furtherance of another crime or tort. This addition would also cover caller ID spoofing done with intent to defraud, as discussed above. Alternatively, for clarity, caller ID spoofing done with intent to defraud may be explicitly included at the felony level. In addition, it may be helpful to provide enhanced penalties for repeat violators. This could lead to greater use of the statute and more just results. Such an approach has been implemented in other federal criminal statutes, including part of the Computer Fraud and Abuse Act, the criminal provision in the Electronic Communications Privacy Act, and 18 U.S.C. 1028(a)(7) (Fraud and related activity in connection with identification documents).

For example, the proposed punishment section could be replaced with the following:

> ***(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State -***
>
> ***(A) be fined under this title or imprisoned for not more than 5 years, or both, in the case of a first offense under this section; and***
>
> ***(B) be fined under this title or imprisoned for not more than 10 years, or both, for any subsequent offense under this section; and***
>
> ***(2) in any other case –***
>
> ***(A) be fined under this title or imprisoned for not more than 1 year or both, in the case of a first offense under this section; and***
>
> ***(B) be fined under this title or imprisoned for not more than 5 years, or both, in the case of an offense under this section that occurs after a conviction of another offense under this section.***

C. Law Enforcement activities should be clearly excepted from the bill's scope.

Proposed section 1040(c) creates an affirmative defense to a prosecution for lawfully authorized activities of law enforcement. Rather than including this exception as an affirmative defense, generally invoked after arrest and indictment, we strongly recommend that proposed section 1040(c) simply exclude this conduct from the statute's

coverage. Thus, we recommend the following language, identical to section 1030(f) of title 18:

> ***(c)*** ~~It is a defense to a prosecution for an offense under this section that the conduct involved was~~ ***This section does not prohibit any*** lawfully authorized investigative, protective or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

D. The bill should include an exception for the blocking of caller ID information.

Unlike the prior legislation addressing the issue of caller ID spoofing, the bill as presently drafted does not include an explicit exception for the blocking of caller ID information, i.e., preventing your number from being known. Caller ID blocking can help protect people's privacy without misleading others and is a standard telephone service feature that has been accepted by the public for decades. The caller gets to make a choice about whether to reveal his or her number and the recipient gets to make a decision about whether to take the call. Although the bill's current language may already allow caller-ID blocking, we suggest adding an exception to the bill that would explicitly preserve caller ID blocking as an option for telephone users.

We suggest the modification of exceptions to read as follows:

> ***"(c) EXCEPTIONS. —***
> ***(1) This section does not prohibit any blocking of caller ID information.***

E. The bill can be made more effective with minor textual edits to the definitions of "caller ID information" and "VOIP service."

As presently drafted, the definition of "caller ID information" included in the bill may be overly expansive; the bill could be read to criminalize the transmittal of false caller ID information other than the information that is transmitted as part of a telephone call. For example, if one person sent an email to another person that contained

information about the origination of an earlier telephone call, it might fall within the bill's definition of "caller ID information." We would therefore recommend rewording the definition to read, "The term 'caller ID information' means ***any identifying*** information regarding the origination of ***a*** telephone call, including the telephone number of the originating party, ***that is transmitted with the call***."

In paragraph (e)(3)(A), the definition of "VOIP service" should include the phrase "***or near-real-time***" in order to address arguments that a service is not real-time simply because of the slight delay inherent in some VOIP services. Culpability for spoofing should be no different simply because the spoofer uses a service with some degree of latency.

V.
Conclusion

The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet this new challenge. Thank you for the opportunity to testify today and for your continuing support. I am happy to answer any questions you may have.