Testimony and Statement for the Record of

Allison Knight
Electronic Privacy Information Center, Staff Counsel

Hearing on

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

Before the

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

Chairman Markey, Ranking Member Upton, and members of the subcommittee, thank you for the opportunity to testify today on caller ID spoofing and H.R. 251, the Truth in Caller ID Act of 2007. My name is Allison Knight and I am Staff Counsel and Director of the Privacy and Human Rights Project at the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. that seeks to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. Thank you for the opportunity to testify before the Subcommittee today.

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

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

EPIC recommended the inclusion of an intent requirement during testimony on a similar bill introduced in the House last year. As Marc Rotenberg, Executive Director of EPIC stated, an intent requirement preserves the privacy rights of callers and permits

legitimate uses of spoofing, while outlawing fraud and harassment assisted by the technology.[1] For example, legitimate law enforcement activity that employs spoofing is preserved by the requirement to show intent to defraud or cause harm, and is therefore adequately addressed within the framework of the proposed legislation as drafted.

Telephone Customers Have Legitimate Reasons to Withhold Their Phone Numbers

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

In the context of the Internet and the offering of voice services over Internet Protocol (VOIP), there are additional concerns about the circumstances under which a person may be required to disclose their identity. The Supreme Court has already made clear that the Internet is entitled to a high level of First Amendment protection.[2]

---

[1] *H.R.5126, the Truth in Caller ID Act of 2006: Before the Subcomm. on Telecommunications and the Internet of the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center)

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

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

In addition to threatening a person's rights to privacy and to freedom of speech, in some circumstances disclosure of a person's phone number may also put his or her safety at risk. For example, domestic violence survivors, shelters, and other safe homes need to preserve the confidentiality of their phone numbers. They may need to contact abusers without exposing their location, in order to arrange custody or other legitimate matters. They may need to contact businesses the abuser is acquainted with, and that may share survivor information with the abuser. They may also need to contact other third parties, such as businesses that have permissive privacy policies, and thus share collected telephone numbers with list or data brokers. In all of these situations, preserving anonymity is necessary for safety.[3]

Caller ID Blocking Does Not Adequately Protect Privacy Interests

Caller ID blocking may seem like a viable means for allowing callers to protect their anonymity while not misleading recipients. However, caller ID blocking is not a complete solution. One reason for this is that caller ID is not the only way that a caller can be identified. Another system, known as Automatic Number Identification, or ANI,

will still disclose a caller's identity in many situations, regardless of whether or not the caller used call blocking. This means that many businesses, emergency service providers, and anyone with a toll-free number can reliably gain the phone number of a caller, even if caller ID is blocked. Spoofing services can protect the anonymity of a caller's ANI data when calling toll-free numbers and those entities that use ANI identification.

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

We also cannot ignore the privacy interests of those who decline to accept calls from unknown numbers. If an individual has been habitually harassed by calls from a caller-ID blocked number, we should not permit the harasser to use spoofing as a means to circumvent the individual's screening. At the same time, it is clear that there could be prosecution for harassment whether or not additional prohibition on spoofing were enacted.[4]

Spoofing Can Create Privacy Risks

This is not to say that caller ID spoofing is an unqualified good--far from it. Last year, EPIC brought to Congress's attention the problem of pretexting consumers' phone records.[5] Pretexting is a technique by which a bad actor can obtain an individual's

---

[3] *Domestic Violence and Privacy*, Electronic Privacy Information Center http://www.epic.org/privacy/dv/.
[4] *See* 47 U.S.C. § 223; 47 U.S.C. § 227.
[5] *Protecting Consumers' Phone Records: Before the Subcomm. on Consumer Affairs, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2006) (statement of Marc Rotenberg, President and

personal information by impersonating a trusted entity. Pretexters have spoofed the telephone numbers of courthouses, in order to harass people for supposedly missing jury duty, threatening fines or arrest unless they turn over social security numbers or other personal information.[6] Rob Douglas of PrivacyToday.com, with whom EPIC has worked on the pretexting issue, noted how fraudsters would use spoofing services in order to fool customers into thinking that fraudulent calls were coming from trusted sources.[7]

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

Significance of NSA Surveillance Program for Privacy of Call Records

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

---

Executive Director, Electronic Privacy Information Center) http://www.epic.org/privacy/iei/sencomtest2806.html; *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?: Before the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center) http://www.epic.org/privacy/iei/pretext_testimony.pdf.

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

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

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

records of American consumers. Last year, EPIC filed a complaint with the Federal Communications Commission in which we alleged that section 222 of the Communications Act, which protects the privacy of customer record information, may have been violated. We urged the Commission to undertake an investigation of this issue.

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

Conclusion

Spoofing caller ID numbers can create a real risk to individuals who might be defrauded or harmed by illegitimate uses of this technology. At the same time, it is important not to punish those who may have a legitimate reason to conceal their actual telephone numbers. By including an intent requirement the revised Truth in Caller ID Act of 2007 distinguishes between appropriate and inappropriate Caller ID spooking and also preserves legitimate law enforcement techniques.

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