Testimony and Statement for the Record of

Marc Rotenberg
President and Executive Director, Electronic Privacy Information Center

Hearing on

H.R. 5126, the Truth in Caller ID Act of 2006

Before the

Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
May 18, 2006
2123 Rayburn House Office Building

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]

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

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

[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.

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 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,

---

[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.

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.

---

[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.

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.

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.