COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL COMMUNICATIONS COMMISSION

In the Matter of "Rules and Regulations Implementing the Truth in Caller ID Act of 2009"

WC Docket No. 11-39

The Federal Communications Commission has requested comment on "Rules and Regulations Implementing the Truth in Caller ID Act of 2009." The Truth in Caller ID Act was signed into law on December 22, 2010.[1] The Truth in Caller ID Act bans the transmission of misleading or inaccurate Caller ID information "with the intent to defraud, cause harm, or wrongfully obtain anything of value."[2] The regulation affects "any real-time voice communications service, regardless of the technology or network utilized."[3]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC also focuses on protecting consumers, and has a particular interest in issues related to the regulation of telemarketing[4] and Caller ID specifically. EPIC testified three times in Congress regarding the Truth in Caller ID Act, before the

[1] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).
[2] *Id.*
[3] *Id.*
[4] *See,* EPIC: Telemarketing and the Telephone Consumer Protection Act, http://epic.org/privacy/telemarketing/default.html.

House of Representatives in 2006[5] and 2007,[6] and before the Senate in 2007.[7] In these various statements, EPIC explained the need to protect both the information provided by the calling party and techniques that could be used to safeguard identity. EPIC specifically recommended the intent requirement that was added to the final bill so that Privacy Enhancing Techniques ("PETs") that would allow some callers to protect the disclosure of their telephone numbers would not be criminalized.

In these comments, EPIC recommends that the FCC amend 47 CFR 64.1601(b), either by eliminating the exemption to toll-free numbers altogether or by prohibiting calls not originally dialed to a toll-free number from being forwarded to a toll-free number with the intent or effect of defeating callers' privacy. This simple change would prohibit third parties from overriding calling parties' privacy choices and safeguard calling information. This change is necessary to ensure that Caller ID Spoofing rules do not impede on a person's legitimate need for to keep his or her telephone number private.

Comments and Recommendations:

Question 27 – Are there ways that carriers and interconnected VoIP providers can prevent third parties from overriding calling parties' privacy choice? If so, would it be appropriate for the Commission to impose such obligations? What is the scope of the Commission's legal authority to address this practice?

[5] Marc Rotenberg, testimony on the Truth in Caller ID Act before the House Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, May 18, 2006, *available at* http://epic.org/privacy/iei/hr5126test.pdf.
[6] Allison Knight, testimony on the Truth in Caller ID Act before the House Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, February 28, 2007, *available at* http://epic.org/privacy/iei/hr251test.pdf.
[7] Allison Knight, testimony on the Truth in Caller ID Act before the Senate Committee on Commerce, Science, and Transportation, June 21, 2007, *available at* http://epic.org/privacy/iei/s704test.pdf.

I. 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 privacy risks.[8] Before these services were offered, telephone customers 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 user 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 order to protect telephone users' right to safeguard the privacy rights of telephone customers, caller ID blocking services were offered. 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.[9] 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.[10] When implementing the initial Caller ID regulations, the Commission preserved a caller's ability to block their phone number from being viewed by the dialed party.[11]

Despite some of the drawbacks to this system (having to pay for permanent

---

8 *See generally* EPIC, "Caller ID," http://epic.org/privacy/caller_id/, and CPSR, "Caller ID," http://epic.org/privacy/caller_id/

9 *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV 1, 4-5.

10 *Id.*

11 FCC Final Rules on Caller ID, 47 CFR 64.1603: "Any common carrier . . . ANI, or charge number on interstate calls must notify its subscribers . . that their telephone number may be identified to a calling party . . must be effecting in informing subscribers how to maintain privacy by dialing *67 on interstate calls.").

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.[12] 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.[13]

Additional concerns arose about the circumstances under which a person may be required to disclose their identity in the context of the Internet and the use of Voice over Internet Protocol (VoIP). VoIP involves the collection of new types of transactional data about the user.[14]

The Supreme Court has repeatedly stated that the First Amendment protects the right to remain anonymous.[15] Internet communications are also entitled to a high level of First Amendment protection. Regulations, therefore, have maintained that all protections available to land-line telephone calls are also available to callers using VoIP technology.[16]

Another problem with requiring callers to disclose the number they call from is

---

[12] Rotenberg testimony, *supra* note 5 at 3-4.
[13] *Id.*
[14] Dr. Richard Kuhn, et al., National Institute of Standards and Technology, Security Considerations for Voice Over IP Systems: Recommendations of NIST, January 2005.
[15] *Watchtower Bible & Tract Society v. Village of Stratton*, 536 U.S. 150 (2002), *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), and *Talley v. California*, 362 U.S. 60 (1960); *ACLU v. Reno*, 521 U.S. 844 (1997).
[16] FCC: Voice-Over Internet Protocol, *available at* www.fcc.gov/voip.

that many individuals 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.

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 at shelters and other safe homes need to preserve the confidentiality of their phone numbers, and thereby prevent the disclosure of their location, in the situation where it is necessary for them to contact abusers, such as to make child-visitation arrangements.[17] These domestic abuse survivors may also need to contact businesses the abuser is acquainted with, and that may share survivor information with the abuser, or other third parties, such as organizations 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 the continued safety of the individual.[18]

Because an individual's choice to block his or her phone number may often be a case of life and death, or at least risk of serious physical injury, the Commission needs to take all appropriate measures to prevent third parties from overriding calling parties' privacy choice.

II. The FCC should amend 47 CFR 64.1601(b) in order to ensure that third parties cannot override calling parties' privacy choice.

[17] Letter from National Network to End Domestic Violence to the House Committee on Energy and Commerce (May 16, 2006).
[18] *Domestic Violence and Privacy*, Electronic Privacy Information Center http://www.epic.org/privacy/dv/.

The Commission asks whether carriers and interconnected VoIP providers can prevent third parties from overriding calling parties' privacy choice. The short answer is simply that they can, but a regulatory change is required, not a technological fix. A provision in the FCC's Caller ID rules, outside the control of carriers and interconnected VoIP providers, is being exploited to destroy callers' privacy.

Current regulations provide that a caller's privacy choice may be ignored when the call is made to a "charge number based service and the call is paid for by the called party" – that is to say, a toll-free number.[19] Companies are abusing this provision to strip privacy from any call, unbeknownst to the caller. This is how it works: A caller dials *67 to avoid passing along her Caller ID information to the call recipient and, in this case, dials the phone number of a customer of a "trapping" service such as TrapCall.[20] TrapCall forwards the call to a toll-free number, where the Caller ID information is obtained. The call, with full Caller ID information, is then re-routed back to the original number dialed.

The original caller did *not* dial a toll-free number, and has no way of knowing that her privacy preference has been completely ignored. The call recipient now has her phone number and, if the recipient subscribes to a top-tier plan, her name and address. The Commission should end this abuse by amending 47 CFR 64.1601(b), either by eliminating the exemption to toll-free numbers altogether, or by prohibiting calls not originally dialed to a toll-free number to be forwarded to a toll-free number with the intent or effect of defeating callers' privacy.

[19] FCC Final Rules on Caller ID, 47 CFR 64.1601(b).
[20] Trap Call, *available at* www.trapcall.com.

Conclusion

EPIC recommends that the FCC amend the FCC's Caller ID rules to eliminate the ability of third parties to exploit the toll-free number provision to defeat callers' privacy. The purpose of the law is to safeguard the identity of the calling party where there is no intent to "defraud, cause harm, or wrongfully obtain anything of value." The Commission should ensure that this intent is protected in the agency's regulations.

Marc Rotenberg
EPIC President

Sharon Goott Nissim
EPIC Consumer Privacy Counsel

Thomas H. Moore
EPIC Of Counsel

Amie Stepanovich
EPIC National Security Counsel