epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

Before the

House Commerce Committee
United States House of Representatives

March 7, 2009
2123 Rayburn House Office Building
Washington, DC

Chairman Dingell, Ranking Member Barton, and Members of the Committee, thank you for the opportunity to testify on the privacy of telephone records and the problem of pretexting. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is non-partisan research organization in Washington, DC that was established to focus public attention on emerging privacy and civil liberties issues. With me this morning is Caitriona Fitzgerald, a student at Northeastern Law School, who has assisted with our testimony.

We thank the Members of the Committee for holding this hearing and for introducing legislation to address the serious problem of pretexting and the associated problem of identity theft. In this statement, I will summarize EPIC's efforts at the FCC to establish stronger security standards for customer information, and express our support for H.R. 936, the bill now before the Committee.

The EPIC Petition to the FCC on Security for Calling Record Information

In the summer of 2005, EPIC undertook an extensive investigation of pretexting. a practice where an individual impersonates another person, employs false pretenses, or otherwise uses trickery to obtain personal information. We found that many web sites were making available personal information that had been wrongfully obtained and that these services were threatening the privacy and security of American consumers. In July 2005, we filed a complaint with the Federal Trade Commission concerning a website that offered phone records and the identities of P.O. Box owners for a fee through pretexting.

We supplemented that filing in August 2005 with a list of 40 websites that offered to sell phone records to anyone online.

In light of the fact that so many companies were selling phone records, EPIC turned to the Federal Communications Commission (FCC) to try to establish better safeguards for phone companies' customer records that were being improperly disclosed. On August 30, 2005, EPIC formally petitioned the FCC to initiate rulemaking for enhance security safeguards for individual's calling records. In our petition, we noted that, through § 222 of the Telecommunications Act of 1996[1], Congress has "specifically placed the burden of protecting Consumer Proprietary Network Information (CPNI) in [telecommunications carriers] hands."[2] Accordingly, the EPIC petition called for the FCC to immediately initiate a rulemaking proceeding to address CPNI protection measures used by telecommunications carriers, and to invite comment to develop adequate safeguards for verifying the identity of parties trying to access CPNI.[3] We suggested five forms of security measures that could be used by telecommunications carriers to more adequately limit disclosure of CPNI.[4]

The telecommunications industry quickly responded to EPIC's petition, suggesting that the FCC take enforcement actions against companies that sell phone records, but opposing any regulatory intervention that would require telecommunications carriers to change their security practices.[5] We responded, pointing out that enforcement

---

[1] 47 U.S.C. § 222 et seq. (2006).
[2] *See* Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) ("EPIC Petition").
[3] *Id.*
[4] *Id.*
[5] *See e.g.* Opposition of BellSouth Corporation to EPIC Petition, RM Docket No. 11277 (filed Oct. 31, 2005).

actions against online data brokers alone was unlikely to prevent the sale of phone records, and that "FCC intervention is necessary to enhance security standards and authentication standards for access to CPNI."[6] The CTIA again responded, asserting that no additional rules were necessary, and suggesting that the FCC deny EPIC's petition to safeguard consumer phone records.[7]

In January 2006, after numerous news reports regarding the vulnerability of phone records to online data brokers, Senator Harry Reid sent a letter to the FCC, urging the agency to "begin an investigation into how online data brokers are obtaining Americans' private phone records, and whether phone companies are doing enough to protect the personal and private information with which they are entrusted." A few days later, on January 17, 2006, FCC Commissioners Adelstein and Copps released statements calling for action to address the illegal sale of telephone records.[8] Commissioner Adelstein noted that EPIC's petition "could be an appropriate vehicle for tightening [the FCC's] rules."[9]

On February 10, 2006, the FCC approved EPIC's petition, seeking comment on the five measures EPIC suggested in order to improve security of CPNI, as well as other measures.[10] The comment deadline was April 14, 2006.

---

[6] Reply Comments of the Electronic Privacy Information Center, CC Docket No. 96-115, RM Docket No. 11277 (Nov. 9, 2005) ("EPIC Reply Comments.")
[7] *See* Reply Comments of CTIA – The Wireless Association to EPIC Reply Comments, CC Docket No. 96-115, RM Docket No. 11277 (Nov. 15, 2005).
[8] Statement by Commissioner Jonathan S. Adelstein on Brokering of Personal Telephone Records (Jan. 17, 2006) ("Adelstein Statement"); Commissioner Michael J. Copps Calls for Action to Address Theft of Phone Records (Jan. 17, 2006) ("Copps Statement").
[9] Adelstein Statement.
[10] *See* 21 F.C.C.R. 1782, 1789 (2006).

FCC Investigation Into Telecommunications Carrier's Security Measures

On September 29, 2006, in a hearing before the House Subcommittee on Oversight and Investigations (Committee on Energy and Commerce), Kris Anne Monteith, Chief of the FCC Enforcement Bureau, discussed the ongoing FCC investigation into phone record security.[11] Chief Monteith asserted in his statement that once the record in the rulemaking proceeding closed in June, FCC Chairman Kevin Martin "directed the staff to expeditiously prepare an order resolving the issues raised in the rulemaking proceeding and intends to bring an order before the full Commission for its consideration this Fall."[12] Despite the apparent urgency of the situation, no such order has yet been promulgated.

All measures the FCC has taken with regard to telecommunications carrier responsibility for CPNI security seem to have taken place prior to its Notice of Proposed Rulemaking. On January 30, 2006, the FCC issued a Public Notice requiring telecommunications carriers to submit CPNI Compliance Certificates.[13] The investigation that followed resulted in the issuance of three "Notices of Apparent Liability for Forfeiture" to telecommunications carriers for failure to comply with CPNI compliance requirements. The FCC has reached consent decrees with two of these three carriers.[14]

---

[11] *See* Written Statement of Kris Anne Monteith, Hearing on "Internet Data Brokers & Pretexting: Who Has Access to Your Private Records?" Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives (Sept. 29, 2006) ("Monteith Statement").

[12] *Id.*

[13] Public Notice re: Enforcement Bureau Directs All Telecommunications Carriers to Submit CPNI Compliance Certificates (January 30, 2006) (available at http://www.fcc.gov/eb/Public_Notices/DA-06-223A1.html.)

[14] Monteith Statement at 5.

According the Chief Monteith, the FCC has also issued formal "Letters of Inquiry" to nearly twenty wireline and wireless carriers.[15] These letters "require the carriers to document their customer data security procedures and practices, identify security and disclosure problems, and address any changes they have made in response to the data broker issue."[16] Analysis of carrier responses is ongoing.

Despite Repeated Statements that CPNI Should be Protected, the FCC has Failed to Issue the Security Guidelines that Would Safeguard Consumer Information

In its Notice of Proposed Rulemaking (Notice), the FCC recognized that its rules implementing § 222 of the Telecommunications Act "require carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[17] It further recognized that Congress granted CPNI the greatest level of protection available under § 222.[18] Thus, the safeguards protecting such information should be such that unauthorized access to it is nearly impossible to accomplish.

However, both the FCC and Congress have recognized that third-party unauthorized access to phone records is a widespread practice. As recently as January 18, 2007, the FCC issued a Consumer Advisory entitled "Protecting the Privacy of Your Telephone Calling Records," explaining to consumers that, despite rules protecting such information, illegal third-party access to phone records is occurring.[19] Congress recently passed legislation making "pretexting" a crime.[20]

---

[15] *Id.*
[16] *Id.*
[17] *Id.* at 1782; *see* 47 U.S.C. § 222(a).
[18] *Id.*
[19] FCC Consumer Advisory, Protecting the Privacy of Your Telephone Calling Records (Jan. 18, 2007) (available at http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html.)
[20] *See* 18 U.S.C §1039 (2006).

Despite the recognition that both CPNI deserves the greatest level of protection available under § 222 due to its highly sensitive nature, and that such information is nonetheless being compromised, the FCC has failed to promulgate regulations to force telecommunications carriers to update its security measures to keep up with the changing technology available to data brokers.

Need for Passage of H.R. 936, Prevention of Fraudulent Access to Phone Records Act

Members of the Committee, Congress passed a law at the end of the last session regarding pretexting, but it addressed only a small part of the problem and did not provide the type of protection that is necessary to safeguard the privacy of American consumers. The Telephone Records and Privacy Protection Act criminalized pretexting but it failed to address the lack of security for telephone records or to resolve the question as to whether the FTC may use its section 5 authority to give after those who traffic in information that is obtained by means of pretexting.[21] The Act amends the federal criminal code to prohibit obtaining, or attempting to obtain, confidential phone records information from a telecommunications carrier (or any covered entity, as defined in § 1039(h)(2)) by: (1) making false or fraudulent statements or representations to an employee of a covered entity; (2) making such false or fraudulent statements or representations to a customer of a covered entity; (3) providing a document to a covered entity knowing that such document is false or fraudulent; or (4)accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section

[21] 18 U.S.C. § 1039.

1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates.[22]

Although Congress' recognition of the seriousness of pretexting, and its efforts to criminalize it, are important, nothing in the law that was passed puts a duty on the telephone companies that are the actual source of this data to increase their security measures. Rather than going after the criminals after the crime occurs, wouldn't it make more sense to reduce the risk that our personal information will be wrongfully disclosed? The proposed Prevention of Fraudulent Access to Phone Records Act addresses the source of the pretexting problem.

Title I of the Act grants enforcement powers over the use of false pretenses to obtain Consumer Proprietary Network Information (CPNI) (a.k.a. pretexting) to the Federal Trade Commission (FTC) by treating it as an unfair or deceptive act or practice prescribed under § 18(a)(1)(B) of the Federal Trade Commission Act.[23] This will resolve any doubt as to the FTC's authority to prosecute these cases.

Title II of the Act establishes the Federal Communications Commission (FCC) provisions. In Section 201, Congress makes clear that telecommunications carriers have a duty to safeguard the confidentiality of its customers personal information.[24] In Section 202, the Act essentially sets forth more detail regarding a telecommunication carrier's obligations to only disclose CPNI to its owner or to authorized users. It prescribes requirements for disclosure of detailed information, requirements for affiliate use of both

---

[22] 18 U.S.C. § 1039(a) (2007). The Act also criminalized the activities of data brokers, prohibiting the sale or transfer of confidential phone records information. § 1039(b). It also makes those who use data broker services criminally liable, prohibiting the act of receiving such information with knowledge that it was illegally obtained. § 1039(c).

[23] H.R. 936, 110th Cong. § 103 (2007).

[24] § 201(2), (10).

general and detailed information, and requirements for partner and contractor use of general information. [25] It further amends § 222(c) of the Communications Act by adding a prohibition of sale, renting, leasing, or otherwise making available of CPNI.[26] Section 203 requires the FCC to prescribe regulations adopting more stringent security standards for CPNI to detect and prevent violations of the Act.[27]

Provisions in the proposed security standards mirror the safeguards suggested by EPIC in our August 2005 petition to the FCC. These measures would greatly benefit CPNI security. However, it should be noted that the only reference to increasing security standards by telecommunications carriers in the required regulations says that a carrier's security policy to should include "appropriate" standards to ensure security. This language does not seem to be much of a shift from the language of the Communications Act, which states that telecommunications carriers have a "duty to protect" CPNI. If carriers have always had a duty to protect such information, it is logical that they have been using "appropriate" standards to ensure such protection all along.

---

[25] § 202(a).
[26] § 202(d).
[27] The regulations that the Act requires the FCC to prescribe are:
(i) to require timely notice to a customer if there is a breach of CPNI regulations relating to his or her information;
(ii) to require timely notice to the FCC if there is a breach of CPNI regulations with respect to any customer;
(iii) to require periodic compliance audits by the FCC of telecommunications carriers;
(iv) to require telecommunications carriers to keep records of each time CPNI is requested, and if access is granted, a note of how the person's identity or authority to access the information was verified;
(v) to require telecommunications carriers to establish a security policy that includes "appropriate" standards to ensure security of CPNI;
(vi) to prohibit the use of pretexting by telecommunications carriers.

§ 203(h)(1)(A).

However, the Act does detail increased more security measures that would improve security of CPNI.[28] The measures it sets forth to consider are: (i) to require telecommunications carriers to "institute customer-specific identifiers in order to access CPNI"; (ii) to require encryption of CPNI (or other safeguards to secure the data); (iii) to require deletion of CPNI after a reasonable period of time if storage is no longer necessary.

These provisions also mirror the security measures suggested by EPIC in its petition to the FCC. If implemented, CPNI security would be significantly stronger. While only requiring the FCC to consider such measures is likely just oft-afforded administrative deference by Congress, given the measures' relative ease of implementation and the risk to privacy that unauthorized access to CPNI entails, it is vital that the FCC act to enforce such protections.

The Prevention of Fraudulent Access to Phone Records Act would provide much needed improved security for CPNI. The information that telephone companies collect and generate about the private activities of their customers should be subject to strong security standards that minimize the risk that individuals will be subject to pretexting and identity theft. CPNI was granted the highest level of protection under the Communications Act – acknowledgment of its extremely sensitive nature. As Congress recognizes in the Act, such information conveys details about the most intimate aspects of an individual's life. Moreover, such information is often used in furtherance of acts of stalking, domestic violence, and other violent crimes. Telephonme

[28] § 203(h)(1)(B).

Conclusion

Mr. Chairman, a year ago I had the privilege to appear before this Committee and to discuss EPIC's efforts to bring attention to the problem of pretexting well before the Hewlett-Packard matter was uncovered. I described our efforts to inform the FTC about this new threat as well as our petition to the FCC to establish stronger security standards for telephone record information. I was heartened at that time by Chairman Martin who expressed concern about the problem of pretexting and indicated that his agency was prepared to act on our petition. In fact, he thanked EPIC for bringing the Commission's attention to the problem.

Here we are now a year later and there has still been no proposal from the FCC to improve the security of the calling information of American consumers. There has been no concerted effort to work with the telephone companies to establish clear guidelines. Moreover, the Chairman has failed to address the question of whether the telephone companies violated the federal Communications Act when they disclosed the records of American citizens to the government without judicial approval. He should open an investigation on this issue as soon as possible.

The privacy provision for telecommunications service in the United States goes back to the original Communications Act of 1934.[29] Privacy protection is critical for consumer trust and confidence in our nation's communications services as well as the success of future communications services. The legislation before the Committee will begin to address the challenges the Commission has been unwilling or unable to.

Thank you for your attention. I will be pleased to answer your questions.

---

[29] § 605.