Order Code RL33287

CRS Report for Congress
Received through the CRS Web

Data Security: Protecting the Privacy of Phone Records

February 28, 2006

Gina Marie Stevens
Legislative Attorney
American Law Division

Tara Alexandra Rainson
Law Librarian
Knowledge Services Group

Data Security: Protecting the Privacy of Phone Records

Summary

The privacy of cellular telephone records has the potential to become a high-priority item on the congressional agenda. The Congress, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), and State Attorneys General are investigating the practices of companies that sell customer calling records for wireless and landline phones to determine whether they are in compliance with current confidentiality protections for customer information. Several federal bills have been introduced to address the breach of phone customers' privacy and to prevent the fraudulent acquisition of telephone records. Hearings have been held in both the House and Senate regarding the sale of phone records, and the House and Senate Judiciary Committees are scheduled to mark up legislation beginning on March 1. The FCC has granted a petition for a rulemaking to determine whether enhanced security and authentication standards for access to customer telephone records are warranted. The FTC is investigating data brokers involved in the practice of selling telephone records and is working with the FCC, which has jurisdiction over telecommunications carriers. At least five states have sued data brokers to enjoin the acquisition and sale of customer records. This report provides a brief discussion of efforts to protect the privacy of customer telephone records. For additional information, see CRS Report RL31636, *Wireless Privacy and Spam: Issues for Congress*, by Marcia S. Smith. This report will be updated when warranted.

Contents

Background 1
Federal Laws 2
Gramm-Leach-Bliley Act 3
Federal Trade Commission Act 3
Customer Proprietary Network Information (CPNI) Under the Communications Act 3
Congressional Response 5
Regulatory Response 7
Litigation 7

Data Security: Protecting the Privacy of Phone Records

Background

According to recent press accounts and a recent petition filed with the Federal Communications Commission (FCC) by the Electronic Privacy Information Center (EPIC), numerous websites advertise the sale of personal telephone records.[1] Specifically, data brokers advertise the availability of cell phone records, which include calls to and from a particular cell phone number, the duration of such calls, and may include the physical location of the cell phone. In addition to selling cell phone call records, many data brokers also claim to provide calling records for landlines and Voice over Internet Protocol (VoIP), as well as nonpublished phone numbers. Data brokers claim to be able to provide this information fairly quickly, in a few hours to a few days.

Although personal information such as Social Security numbers can be found on public documents, phone records are stored only by phone companies.[2] For this reason, data brokers are alleged to have obtained phone records from the phone companies themselves, albeit without their approval. It is also believed that data brokers have taken advantage of inadequate company security standards to gain access to customer telephone information. Data brokers are thought to employ three different practices to obtain customer telephone records without the approval of the customer. The first method occurs when an employee of one of the phone companies sells the records to the data broker. The second method occurs through a practice called "pretexting," where a data broker pretends to be the owner of the phone and obtains the records from the telephone company under false pretenses. The third method is employed when a data broker obtains the customer's telephone records by accessing the customer's account on the Internet.

Phone companies are believed to have strict rules preventing and guarding against the employee sale of telephone records and the unauthorized acquisition of customer information. On the other hand, private investigators, often routine users of telephone customer record data, state that information security by carriers to protect customer records is practically nonexistent and is routinely defeated. The

---

[1] 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), at [http://www.epic.org/privacy/iei/].

[2] Jonathan Krim, "Online Data Gets Personal: Cell Phone Records for Sale," *Washington Post*, July 8, 2005, at D01.

Federal Trade Commission (FTC) has indicated that data-theft investigations have shown that "finding someone on the inside to bribe is not that difficult."[3]

Pretext calling for customer telephone records occurs when the data broker or investigator pretends to be the cell phone account holder and persuades phone company employees to release the information. The public availability of personal identifiers, like the Social Security number, makes it easier for someone to impersonate the account holder to convince the employee that they are the account holder.

Telephone companies are encouraging customers to receive electronic statements and to access customer accounts online. Typically, online accounts are set up in advance, to be activated at a later date by the customer. If someone can figure out how to activate and access the online account of the customer, the call records can be obtained.

With respect to the issue of who is purchasing the phone records from data brokers, EPIC recently investigated this question and concluded that attorneys are among the top users of private investigators and pretexting. In response to its finding, EPIC wrote to State Bar Ethics Committees, noting that "it has become increasingly clear that attorneys are major consumers of pretexting services. In this letter, we request that appropriate action be taken to ensure that attorneys in your state are not employing investigators or other companies to engage in pretexting or other fraud."[4]

Federal Laws

Although there is no single federal law governing data brokers, other statutes and regulations may be applicable. A review of the laws regulating use and disclosure of information collected by information brokers appears in CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie A. Welborn. Certain sectors are currently subject to legal obligations to protect sensitive personal information. These obligations were created, in large part, through the enactment of federal privacy legislation in the financial services, health care, government, and Internet sectors. Federal regulations issued to carry out requirements of federal privacy laws impose obligations on covered entities to implement information security programs to protect personal information. For further information, see CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

---

[3] *Federal Legislation Introduced to Stop the Sale of Phone Records*, (Jan. 20, 2006) at [http://www.govtech.net/magazine/channel_story.php/97955].

[4] Electronic Privacy Information Center, *Letter to Ethics Board Concerning Attorneys' Use of Pretexting* (Feb. 21, 2006) at [http://www.epic.org/privacy/iei/attyltr22106.html#_ftn1].

Although pretext calling for financial information is illegal, telephone records are not included in this prohibition.[5] Several federal statutes address illegal conduct associated with identity theft and pretext calling.[6]

Gramm-Leach-Bliley Act. Section 523 of the act makes it a crime to obtain customer information of a financial institution by means of false or fraudulent statements to an officer, employee, or agent or customer of a financial institution, or to request another person to obtain customer information from a financial institution if the requester knows that the information will be obtained by making a false or fraudulent statement.[7]

Federal Trade Commission Act. The FTC may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices.[8] Using its authority under Section 5, the FTC has brought a number of cases against businesses that use pretexting to gather financial information on consumers. Currently, the FTC is investigating data brokers that use pretexting to gather customer telephone records and is working with the FCC, which has jurisdiction over telecommunications carriers subject to the Communications Act. In addition, the FCC is investigating telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of customer data, and it has initiated a proceeding to determine what additional rules it should adopt to protect phone records from unauthorized disclosure.

Customer Proprietary Network Information (CPNI) Under the Communications Act. Section 222 of the Communication Act of 1934, as amended, establishes a duty of every telecommunications carrier to protect the confidentiality of its customers' customer proprietary network information (CPNI).[9] CPNI includes personally identifiable information derived from a customer's relationship with a telephone company, irrespective of whether the customer purchases landline or wireless telephone service. CPNI is defined as

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer

---

[5] See CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[6] Board of Governors of the Federal Reserve System, *Identity Theft and Pretext Calling*, Apr. 26, 2001, at [http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0111.htm].

[7] 15 U.S.C. § 6828.

[8] 15 U.S.C. §§ 41-58.

[9] 47 U.S.C. § 222. Section 222 was added to the Communications Act by the Telecommunications Act of 1996. Telecommunications Act of 1996, P.L. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 et seq.)

> relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.[10]

In section 222, Congress created a framework to govern telecommunications carriers' use of information obtained through provision of a telecommunications service. Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information of other carriers, equipment manufacturers, and customers.[11] Section 222(b) states that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may use such information only for that purpose and may not use that information for its own marketing efforts.[12] Section 222(c) establishes the confidentiality protections applicable to customer information. Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to customers' individually identifiable CPNI in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service. Section 222(c)(2) provides that a carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[13] Section 222(c)(3) provides that a carrier may use, disclose, or permit access to aggregate customer information other than for the purposes described in subsection (1). Section 222(d) delineates certain exceptions to the general principle of confidentiality.[14] Section 222(e) addresses the disclosure of subscriber list information.

The FCC's regulations implementing Section 222 govern the use and disclosure of customer proprietary network information by telecommunications carriers.[15] When the FCC implemented Section 222, telecommunications carriers were required to obtain express written, oral, or electronic consent from their customers (i.e., "opt-in consent") before a carrier could use customer phone records to market services outside of the customer's relationship with the carrier.

The United States Court of Appeals for the Tenth Circuit struck down those rules, finding that they violated the First and Fifth Amendments of the Constitution.[16] In that case, the plaintiffs argued that the regulations adopted by the CPNI Order constituted an arbitrary and capricious interpretation of Section 222. In response to the decision, the FCC reversed its opt-in requirement and implemented an opt-out rule; telecommunications carriers must receive opt-in (affirmative) consent before disclosing CPNI to third parties or affiliates that do not provide

---

[10] 47 U.S.C. § 222(h)(1).

[11] 47 U.S.C.§ 222(a).

[12] 47 U.S.C. § 222(b).

[13] 47 U.S.C. § 222(c).

[14] 47 U.S.C. § 222(d).

[15] 47 C.F.R. §§ 64.2005 - § 64.2009.

[16] *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), cert. denied *Competition Policy Instit. v. U.S. West, Inc.*, 530 U.S. 1213 (2000).

communications-related services.[17] However, telecommunications carriers are permitted to disclose CPNI to their joint venture partners and independent contractors that provide communications-related services after obtaining a customer's "opt-out" consent.[18] Carriers are also required by the rules to establish safeguards to protect against unauthorized disclosure of CPNI, including requirements that carriers maintain records that track access to customer CPNI records. Each carrier is also required to certify annually its compliance with the CPNI requirements and to make this certification publicly available.

In sum, telecommunications carriers are subject to clear and unambiguous obligations to guard the confidentiality of CPNI and to ensure that it is not disclosed to third parties without customer approval or as required by law.

Congressional Response

The House Energy and Commere Committee held a hearing on February 1, 2006,[19] and the Senate Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance held a hearing on February 8, 2006.[20] Legislation has also been introduced that seeks to improve safeguards over customers' records.[21] The House Judiciary Committee plans to mark up H.R. 4709 on March 1, and the Senate Judiciary Committee plans to mark up S. 2178 on March 2. Draft bills are reportedly circulating in the House Energy and Commerce Committee and the Senate Commere, Science, and Transportation Committee to target the sale of phone records by data brokers. The House Energy and Commerce Committee has launched an investigation into website operators that sell customers phone records.

H.R. 4662, Consumer Telephone Records Protection Act of 2006 (Blackburn). This bill prohibits the obtaining of telephone records by false pretenses and the selling or disclosure of records obtained by false pretenses. False pretenses include making a false statement to a telecommunications carrier or providing any information to a telecommunication carrier knowing that it is false or that it was obtained fraudulently or without the customer's consent. The bill also requires that a carrier notify a customer when the customer's records are disclosed

---

[17] Except as required by law, carriers may not disclose CPNI to third parties or their own affiliates that do not provide communications-related services unless the consumer has given "opt in" consent, which is express written, oral, or electronic consent. 47 C.F.R. §§ 64.2005(b), 64.2007(b)(3); 64.2008(e); see also 47 C.F.R. § 64.2003(h) (defining "opt-in approval").

[18] 47 C.F.R. §§ 64.2005(b), 64.2007(b)(1).

[19] *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting? Hearing Before the House Comm. on Energy and Commerce*, 109th Cong., 2nd Sess. (Feb. 10, 2006).

[20] *Protecting Consumers' Phone Records, Hearing Before the Subcomm. on Consumer Affairs, Product Safety, and Insurance of the Senate Comm. on Commerce, Science, and Transportation*, 109th Cong., 2nd Sess. (Feb. 8, 2006).

[21] Bill summaries prepared by Tara A. Rainson, Law Librarian, Congressional Research Service, Knowledge Services Group.

to someone other than the customer. A violation would be treated as a violation of the Federal Trade Commission Act. All powers and functions of the FTC under that act are available to enforce compliance. Prescribed penalties include a fine, up to five years imprisonment, or both. Penalties are doubled for offenses that involve more than $100,000 or more than 50 customers in a 12-month period, or take place while violating another federal law.

H.R. 4678, Stop Attempted Fraud Against Everyone's Cell and Land Line (SAFE CALL) Act (Schakowsky). This bill prohibits the obtaining of telephone records by false pretenses and the selling or disclosing of records obtained by false pretenses. False pretenses include making a false statement to a telecommunications carrier or providing any information to a telecommunication carrier knowing that it is false or that it was obtained fraudulently or without the customer's consent. A violation would be treated as a violation of the Federal Trade Commission Act. All powers and functions of the FTC under that act are available to enforce compliance. No new penalties established.

H.R. 4709, Law Enforcement and Phone Privacy Protection Act of 2006 (Smith) amends the federal criminal code to prohibit the obtaining by fraud or other unauthorized means of confidential phone records information from a telecommunications carrier or IP-enabled voice service provider (covered entity); the unauthorized sale or transfer of such records by any person, including any employee of a covered entity; and the purchase of such records with knowledge that they were fraudulently obtained or obtained without authorization. This bill exempts lawful requests for information by law enforcement agencies. Penalties include a fine and/or imprisonment for up to 20 years and increases in applicable penalties for violations occurring in a 12-month period involving more than $100,000 or more than 50 customers of a covered entity, and for violations involving the use of confidential phone records information in furtherance of certain crimes of violence. The bill directs the U.S. Sentencing Commission to review and amend, if appropriate, federal sentencing guidelines and policy statements for the crimes defined by this act.

H.R. 4714, Phone Records Protection Act of 2006 (Boswell) amends the federal criminal code to prohibit the intentional sale or fraudulent transfer or use of the records of a customer or a telephone service provider. Telephone service means any form of telecommunications service as defined in 47 U.S.C. §153 (46). Telephone service also includes any form of wireless phone service, including cellular phones, broadband, and specialized mobile radio service. Penalties include a fine, up to 10 years imprisonment, or both. An exception is made for providing customer records to law enforcement.

S. 2177, Phone Records Protection Act of 2006 (Durbin). This bill prohibits the sale or fraudulent use of the records of a customer of a telephone service provider. Telephone service means any form of telecommunications service as defined in 47 U.S.C. §153 (46). Telephone service also includes any form of wireless phone service, including cellular phones, broadband, and specialized mobile radio service. The bill makes an exception for law enforcement agencies that seek to obtain telephone records in connection with official law enforcement duties. It imposes a fine, up to 10 years imprisonment, or both.

S. 2178, Consumer Telephone Records Protection Act of 2006 (Schumer). This bill amends the federal criminal code to prohibit obtaining confidential phone records information by fraud or by any other unauthorized means. The bill also prohibits the sale of these records. The bill applies to the records of any telecommunications carrier or IP-enabled voice service provider. An exception is provided for law enforcement agencies that seek to obtain telephone records in connection with official duties. The bill imposes a fine, up to five years imprisonment, or both. Penalties are doubled for violations occurring in a 12-month period that involve more than $100,000 or the records of more than 50 telephone service customers.

Regulatory Response

The FCC launched a proceeding on February 10, 2006, *Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information*, to determine whether enhanced security and authentication standards for access to customer telephone records are warranted. [22] In a Notice of Proposed Rulemaking (NPRM), the Commission seeks comment on a variety of issues related to customer privacy, including what security measures carriers currently have in place, what inadequacies exist in those measures, and what kind of security measures may be warranted to better protect consumers' privacy.[23] The NPRM grants a petition for rulemaking filed by the Electronic Privacy Information Center (EPIC) expressing concerns about whether carriers are adequately protecting customer call records and other customer proprietary network information, or CPNI. In its petition, EPIC proposed five additional security measures to more adequately protect CPNI. The NPRM specifically seeks comment on these five measures, which are (1) passwords set by consumers; (2) audit trails that record all instances when a customer's records have been accessed and whether information was disclosed, and to whom; (3) encryption by carriers of stored CPNI data; (4) limits on data retention that require deletion of call records when they are no longer needed; and (5) notice provided by companies to customers when the security of their CPNI may have been breached.

Litigation

In January 2006, a federal district judge in Georgia blocked online data broker First Source Information Specialist, Inc. from selling the illegally obtained phone records of Cingular Wireless customers. The complaint stated that the

> [d]efendants wrongfully obtain and disseminate confidential customer information, such as a customer's call records, through fraud and deception by engaging in "social engineering," improper hacking, and/or unauthorized access

---

[22] Federal Communications Commission, *FCC Examines Need For Tougher Privacy Rules: Comment Sought On Measures Proposed by EPIC*, (Feb. 10, 2006), available at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263765A1.pdf].

[23] Federal Communications Commission, *Notice of Proposed Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket No. 96-115 (Feb. 10, 2006), available at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-10A1.pdf].

> to online account information stored on Cingular's computer network. For example, Defendants or their agents call Cingular's customer service representatives and dishonestly pose as customers seeking information about his or her own account, pose as fellow employees facing an urgent access problem in accessing a customer account, and/or access customers' online accounts fraudulently, using customers' passwords without their knowledge or consent.[24]

The complaint alleged fraud, conversion of property, unfair and deceptive acts and practices, civil conspiracy, replevin, intentional access of a protected computer system without authorization in violation of the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(2)c)), knowingly and with intent to defraud access of a protected computer system without authorization and/or in excess of authorized access and obtaining without authorization customer information the value of which exceeds $5000 in any one-year period in violation of the federal Computer Fraud and Abuse Act (18 U.S.C. § (a)(4)(g)), and trespass to chattels.

The federal district court determined that Cingular had shown a substantial likelihood of success on the merits with respect to the fraud claim and granted Cingular's motion for a temporary restraining order. The court enjoined the defendants from attempting to obtain information from Cingular regarding any of its customers; using the name or identity of any Cingular employee or customer; contacting Cingular; providing Cingular customer information in their possession to third parties; advertising that defendants can or will obtain information regarding wireless telephone subscribers; possessing confidential information obtained from Cingular; and disposing of any confidential Cingular customer information.

At least five states (Florida, Illinois, Missouri, Connecticut, and Texas) have brought suits against individual information brokers. In Florida, a suit was brought against First Source Information Specialist, Inc. (doing business as locatecell.com, celltolls.com, datafind.org, and peoplesearchamerica.com), located in Tamarac, Florida, the same company sued by Cingular.[25] The state sued for deceptive trade violations in obtaining and selling phone call records through the company's Internet sites and is seeking a $50 million fine — $10,000 for each of the 5,000 alleged transactions in which employees of the data broker impersonated phone company customers or employees to get copies of people's phone records.[26] Florida has brought another suit against a second data broker, alleging that it obtained

---

[24] *Complaint of Cingular in Cingular Wireless LLC v. Data Find Solutions, Inc., James Kester, 1st Source Information Specialists, Inc., Kenneth W. Gorman, Steven Schwartz, John Does 1-100,and XYZ Corps. 1-100*, Docket No. 1 05-CV 3269-CC (D.N.D. Ga. filed Dec. 23, 2005) (Cingular Petition). In addition to the Cingular lawsuit, Verizon Wireless has also sued data brokers, claiming they posed as customers to obtain private calling records and then advertised and sold the phone call records on the Internet. See, e.g., *Cellco Partnership d/b/a/ Verizon Wireless v. Source Resources*, Permanent Injunction on Consent, Docket No. SOM-L-1013-05 (Sup. Ct. of N.J.; Law Div.: Somerset County, Sept. 13, 2005).

[25] *Fla. v. IST Source Information Specialists, Inc*. (2006), available at [http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6L8KGC/$file/1stSource_Complaint.pdf].

[26] C. B. Hanif, "Private Information, Too Many Prying Eyes," *Palm Beach Post*, 1E (Jan. 29, 2006).

information by impersonating either customers or telephone company employees to obtain consumers' personal calling information.[27] Illinois also filed suit against First Source Information Specialist, Inc.[28] In response to a suit filed by the Missouri attorney general, a Missouri judge prohibited Completeskiptrace.com from obtaining or selling the cell phone records of Missourians. Missouri also obtained a preliminary injunction against Locatecell.com, an Internet business that sells cell phone records, from conducting business in the state.[29] The Texas Attorney General has filed suit against a "data broker" and his companies — USA Skiptrace, AMS Research Services Inc., and Worldwide Investigations Inc. — for fraudulently marketing consumers' private phone records.[30]

Some State Attorneys General have begun investigations into data brokers that sell phone records. The state of Connecticut has launched an investigation into several specific companies that obtain and sell personal cellular phone records, including a listing of calls consumers make from their phones.[31] The Massachusetts Attorney General issued letters to Cingular Wireless, Sprint, T-Mobile, U.S. Cellular, and Verizon requesting that the cell phone companies "discuss with us your policies and practices regarding access to billing and other account information via telephone and online."

---

[27] *Fla. v. Global Information Group*, (2006), available at [http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6M9RY3/$file/Global_Complaint.pdf].

[28] Office of the Illinois Attorney General, *Madigan Sues Company That Buys Cell Phone Records: Attorney General Calls Abuse "Privacy Theft*," (Jan. 20, 2006), available at [http://illinoisattorneygeneral.gov/pressroom/2006_01/20060120.html].

[29] Missouri Attorney General's Office, *Court Orders Web Business to Stop Obtaining, Selling Cell Phone Records of Missourians*, (Feb. 23, 2006) available at [http://www.ago.mo.gov/newsreleases/2006/022306c.htm].

[30] Attorney General of Texas, *Attorney General Abbott Files First Suit Against Sellers Of Private Phone Records*, (Feb. 9, 2006), available at [http://www.oag.state.tx.us/oagnews/release.php?id=1449&PHPSESSID=qg0f5ul9clscml5e685r4n9dn7].

[31] State of Connecticut Attorney General's Office, *Attorney General Continues Investigating Companies Selling Personal Cell Phone Records*, (Jan. 18, 2006), available at [http://www.ct.gov/ag/cwp/view.asp?A=2426&Q=308758].