Order Code RL33287

CRS Report for Congress
Received through the CRS Web

Data Security: Protecting the Privacy of Phone Records

Updated May 17, 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 become a high-priority item on the congressional agenda. According to recent press accounts, numerous websites advertise the sale of personal telephone records. In addition, recent media disclosures regarding an alleged National Security Agency (NSA) program designed to collect and analyze information on telephone calling patterns within the United States has raised interest in the means by which the government may collect phone records. For further information, see CRS Report RL33424, *Government Access to Phone Calling Activity and Related Records: Legal Authorities.*

Hearings have been held in both the House and Senate regarding the sale of phone records. Several bills have been introduced to address the breach of phone customers' privacy and to prevent the fraudulent acquisition of telephone records (H.R. 4657, H.R. 4662, H.R. 4678, H.R. 4709, H.R. 4714, H.R. 4943, S. 2177, S. 2178, and S. 2389). Generally, the bills follow one of two legislative approaches. The first approach prohibits the practice of pretexting to obtain confidential customer information, expands the enforcement authority of the FTC, and requires the FCC to issue rules to implement information security programs (e.g., H.R. 4943, S. 2389). The second approach would create new criminal penalties for fraudulently obtaining and disclosing phone records (e.g., H.R. 4709, S. 2178).

H.R. 4709 was reported by the House Judiciary Committee and passed by the House, 409-0, on April 25. The Senate Judiciary Committee reported S. 2178, which is nearly identical to H.R. 4709. The House Energy and Commerce Committee reported H.R. 4943. The House was scheduled to consider H.R. 4943 on May 2, but the bill was removed from the floor schedule because of jurisdictional concerns in the House Intelligence Committee. The Senate Commere, Science, and Transportation Committee reported S. 2389. Senate Majority Leader Frist has directed the Senate Commerce and Judiciary Committees to work together on a bill.

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 has filed complaints charging five Web-based businesses with violating the Federal Trade Commission Act. At least five State Attorneys General have also sued data brokers to enjoin the acquisition and sale of customer records.

This report discusses recent legislative and regulatory efforts to protect the privacy of customer telephone records, and efforts to prevent the unauthorized use, disclosure, or sale of such records by data brokers. In addition, it provides a brief overview of the confidentiality protections for customer information established by the Communications Act of 1934. It does not discuss the legal framework for the disclosure by telephone companies of phone records to the government. For an overview of federal law governing wiretapping and electronic eavesdropping, see CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*. This report will be updated when warranted.

Contents

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 landline and Voice over Internet Protocol (VoIP) phones, 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.

The Federal Trade Commission has filed federal court complaints in Maryland, Wyoming, Florida, California, and Virginia charging five Web-based operations that have obtained and sold consumers' confidential telephone records to third parties with violating Section 5(a) of Federal Trade Commission Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The agency is seeking a permanent halt to the sale of the phone records and a rescission of contracts, restitution, disgorgement of ill-gotten gains, and other equitable relief.[9]

The Communications Act. Telecommunications carriers are subject to obligations to guard the confidentiality of customer proprietary network information (CPNI) and to ensure that it is not disclosed to third parties without customer approval or as required by law. Section 222 of the Communication Act of 1934, as amended, establishes a duty of every telecommunications carrier to protect the confidentiality of CPNI.[10] Section 222 attempts to achieve a balance between marketing and customer privacy.

---

[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] FTC Seeks Halt to Sale of Consumers' Confidential Telephone Records, May 3, 2006, at [http://www.ftc.gov/opa/2006/05/phonerecords.htm].

[10] 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.)

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 relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.[11]

CPNI includes customers' calling activities and history (e.g., phone numbers called, frequency, duration, and time), and billing records. It does not include subscriber list information, such as name, address, and phone number.

In section 222, Congress created a framework to govern telecommunications carriers' use of information obtained through provision of a telecommunications service. Section 222 of the Act provides that telecommunications carriers must protect the confidentiality of customer proprietary network information. The Act limits carriers' abilities to use customer phone records, including for their own marketing purposes, without customer approval and appropriate safeguards. The Act also prohibits carriers from using, disclosing, or permitting access to this information without the approval of the customer, or as otherwise required by law, if the use or disclosure is not in connection with the provided 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.[12] 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.[13]

The confidentiality protections applicable to customer proprietary network information are established in section 222(c). Subsection (c)(1) constitutes the core privacy requirement for telecommunications carriers.

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the

---

[11] 47 U.S.C. § 222(h)(1).

[12] 47 U.S.C.§ 222(a).

[13] 47 U.S.C. § 222(b).

> provision of such telecommunications service, including the publishing of directories.[14]

A carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[15] 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).[16] Thus, the general principle of confidentiality for customer information is 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.

Exceptions to the general principle of confidentiality permit carriers to use, disclose, or permit access to customer proprietary network information to (1) initiate, render, bill, and collect for telecommunications services; (2) protect the rights or property of the carrier, the customers, and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (3) provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call; and (4) provide call location information concerning the user of a commercial mobile service for emergency.[17]

Section 222(e) addresses the disclosure of subscriber list information and permits carriers to provide subscriber list information to any person upon request for the purpose of publishing directories. The term "subscriber list information" means any information identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications, or any combination of such listed names, numbers, addresses, or classifications; that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.[18]

Customer Proprietary Network In formation (CPNI) Regulations. In 1998, the Federal Communications Commission issued its *CPNI Order* to implement section 222.[19] The *CPNI Order* and subsequent orders issued by the Commission govern the use and disclosure of customer proprietary network information by telecommunications carriers. When the FCC implemented Section 222, telecommunications carriers were required to obtain express consent from their customers (i.e., "opt-in consent") before a carrier could use customer phone records

---

[14] 47 U.S.C. § 222(c)(1).

[15] 47 U.S.C. § 222(c)(2).

[16] 47 U.S.C. § 222(c)(3). The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. 47 U.S.C. § 222(h)(2).

[17] 47 U.S.C. § 222(d).

[18] 47 U.S.C. § 222(e).

[19] *CPNI Order*, 13 FCC Rcd 8061.

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.[20]

Current CPNI regulations require telecommunications carriers to receive opt-in (affirmative) consent before disclosing CPNI to third parties or affiliates that do not provide communications-related services.[21] However, carriers are permitted to disclose CPNI to affiliated parties after obtaining a customer's "opt-out" consent.[22] "Opt-Out" consent means that the telephone company sends the customer a notice saying it will consider the customer to have given approval to use the customer's information for marketing unless the customer tells it not to do so (usually within 30 days.)[23] Carriers are required, prior to soliciting the customer's approval, to provide notice to the customer of the customer's right to restrict use, disclosure, and access to the customer's CPNI.[24] Carriers are also required to establish safeguards to protect against the unauthorized disclosure of CPNI, including requirements that carriers maintain records that track access to customer CPNI records.[25] Each carrier is also required to certify annually its compliance with the CPNI requirements and to make this certification publicly available.[26] The FCC recently proposed $100,000 fines on telephone companies with inadequate certifications regarding compliance with FCC rules protecting customer information from disclosure.[27]

Penalties. Carriers in violation of the CPNI requirements are subject to a variety of penalties under the Act.

Carriers in violation of the CPNI requirements are subject to a variety of penalties under the Act. Under the criminal penalty provision in section 501 of the Act, 47 U.S.C. § 501, any person who willfully and knowingly does, causes or allows to be done, any act, matter, or thing prohibited by the Act or declared unlawful, or who willfully and knowingly omits or fails to do what is required by the Act, or who willfully or knowingly causes or allows such omission or failure, shall be punished for any such offense for which no penalty (other than a forfeiture) is provided by the

---

[20] *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).

[21] 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").

[22] 47 C.F.R. §§ 64.2005(b), 64.2007(b)(1).

[23] FCC Consumer Advisory: Protecting the Privacy of Your Telephone Calling Records, at [http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html].

[24] 47 C.F.R. §§ 64.2008.

[25] 47 C.F.R. §§ 64.2009.

[26] 47 C.F.R. §§ 64.2009(e).

[27] In the Matter of Cbeyond Communications, LLC, 2006 FCC LEXIS 1902, April 21, 2006, at [http://www.fcc.gov/eb/Orders/2006/DA-06-916A1.html].

Act by a fine up to $10,000, imprisonment up to one year, or both, and in the case of a person previously convicted of violating the Act, a fine up to $10,000 imprisonment up to two years, or both.

Section 502 of the Act punishes willful and knowing violations of Federal Communication Commission regulations. Any person who willfully and knowingly violates any rule, regulation, restriction, or condition made or imposed by the Commission is, in addition to other penalties provided by law, subject to a maximum fine of $500 for each day on which a violation occurs.[28]

Under section 503(b)(1) of the Act, any person who is determined by the Commission to have willfully or repeatedly failed to comply with any provision of the Act or any rule, regulation, or order issued by the Commission shall be liable to the United States for a civil money "forfeiture" penalty.[29] Section 312(f)(1) of the Act defines "willful" as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate" the law. "Repeated" means that the act was committed or omitted more than once, or lasts more than one day. If the violator is a common carrier, section 503(b) authorizes the Commission to assess a forfeiture penalty of up to $130,000 for each violation or for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,325,000 for any single act or failure to act.[30] To impose such a forfeiture penalty, the Commission must issue a notice of apparent liability, and the person against whom the notice has been issued must have an opportunity to show, in writing, why no such forfeiture penalty should be imposed. The Commission will then issue a forfeiture if it finds by a preponderance of the evidence that the person has violated the Act or a Commission rule.

Federal Communications Commission Regulatory Actions. The FCC is examining telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of customer data. 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. [31] 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.[32]

---

[28] 47 U.S.C. § 502.

[29] 47 U.S.C. § 503(b)(1).

[30] FCC Forfeiture Proceedings, Limits on the amount of forfeiture assessed, 47 C.F.R. Part 1.80(b).

[31] 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].

[32] Federal Communications Commission, *Notice of Proposed Rulemaking to Enhance* (continued...)

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.

Comments in opposition to the proposed FCC rulemaking were filed by several telecommunications carriers in the industry that believe the issue can best be addressed using existing laws.[33] Comments were filed with the FCC by the United States Telecom Association, the National Telecommunications Cooperative Association, the National Cable & Telecommunications Association, Time Warner Telecom, Inc., the Cellular Telecommunications Industry Association, the Rural Cellular Association, and T-Mobile USA, Inc. Consumer groups such as the National Association of State Utility Consumer Advocates were generally supportive of EPIC's proposal. Public Utility Commissions, California and Texas, also urged the adoption of strict rules to protect consumer privacy.

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 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.[34]

---

[32] (...continued)
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].

[33] "Telcos Urge FCC to Shelve Bid For New CPNI Rules, *TR Daily*, May, 1, 2006.

[34] *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 (continued...)

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.[35] 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.[36] Florida has brought another suit against a second data broker, alleging that it obtained information by impersonating either customers or telephone company employees to obtain consumers' personal calling information.[37] Illinois also filed suit against First Source Information Specialist, Inc.[38] In response to a suit filed by the Missouri

---

[34] (...continued)
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).

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

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

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

[38] 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 (continued...)

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.[39] 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.[40]

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.[41] 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."[42]

Congressional Response

The House Energy and Commere Committee held a hearing on February 1, 2006,[43] and the Senate Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance held a hearing on February 8, 2006.[44] In addition, the House Energy and Commerce Committee has launched an investigation into website operators that sell customers' phone records.

Legislation has also been introduced that seeks to improve safeguards over customers' phone records. The House Judiciary Committee reported H.R. 4709 on March 16, and the House passed H.R. 4709 on April 25, 409-0. The Senate Judiciary Committee reported S. 2178 on March 2 without written report. The House Energy and Commerce Committee reported H.R. 4943 with report on March 16, and the

---

[38] (...continued)
[http://illinoisattorneygeneral.gov/pressroom/2006_01/20060120.html].

[39] 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].

[40] 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].

[41] 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].

[42] The Office of the Massachusetts Attorney General, *AG Reilly Calls on Cell Phone Companies to Secure Consumer Information*, Feb. 9, 2006, available at [http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1603].

[43] *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).

[44] *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).

Senate Commere, Science, and Transportation Committee reported S. 2389 on March 30.[45] The House was scheduled to consider H.R. 4943 on May 2, but the bill was removed from the floor schedule because of jurisdictional concerns in the House Intelligence Committee.[46]

Generally, the bills follow one of two legislative approaches for the protection of phone records. The first approach prohibits the practice of pretexting to obtain confidential customer information, expands the enforcement authority of the FTC, and requires the FCC to make sure that telecommunications carriers protect the privacy of customer records (e.g., H.R. 4943, S. 2389). The second approach would create new criminal penalties for fraudulently obtaining and disclosing phone records (e.g., H.R. 4709, S. 2178).

Several issues of contention remain to be resolved. These include preemption of state laws (S. 2389), prohibition on the dissemination of cell phone numbers from telephone directories by phone companies without the prior written consent of subscribers (S. 2389, H.R. 4943), requirement for consumer opt-in to the bill's protections (H.R. 4943), creation of a private right of action in federal court for individuals against those who fraudulently obtain their phone records (S. 2389), and exceptions for intelligence agencies. An additional consideration for the Senate is whether it will take up the Judiciary (S. 2178) and Commerce (S. 2389) bills separately, as the House did, or combine them into a single measure. Senate Majority Leader Frist has directed the Senate Commerce and Judiciary Committees to work together on a bill.

H.R. 4657, Secure Telephone Operations Act of 2006 (Lipinski) amends the federal criminal code to prohibit the sale of telephone customer proprietary network information.

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 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.

---

[45] Libby George, "Senate Panel Amendment Could Hang Up Cell Phone Records Protection Bill," *CQ Today*, March 30, 2006.

[46] Seth Stern, GOP Leaders Pull Telephone Records Fraud Bill From House Floor Schedule, *CQ Today*, May 1, 2006.

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). H.R. 4709 was reported by the House Judiciary Committee (H.Rept. 109-395) on March 16, 2006, and passed by the House on April 25.[47] It amends the federal criminal code to prohibit the obtaining by fraud or other unauthorized means of confidential phone records information of a consumer 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 lawfully authorized investigative, protective, or intelligence activities of a law enforcement or intelligence agency. Penalties for the crime of obtaining confidential information from a covered entity by fraud include a fine for individuals up to $250,000 and up to $500,000 for companies, and/or imprisonment for up to 20 years. Similar fines are imposed for the sale, transfer, or attempts to sell or transfer such records without authorization and for individuals who purchase confidential phone records information knowing the records were obtained without authorization. For the latter two offenses, imprisonment up to five years may also be imposed. Enhanced penalties are provided for violations occurring in a 12-month period involving more than $100,000 or more than 50 customers of a covered entity. The legislation allows for enhanced penalties for cases in which the information is used to commit further crimes, is used to further a crime of violence, or causes substantial financial harm. 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.

H.R. 4943, Prevention of Fraudulent Access to Phone Records Act (Barton). H.R. 4943 was reported by the House Energy and Commerce (H.Rept.

---

[47] *Law Enforcement and Phone Privacy Protection Act of 2006: Report of the House Committee on the Judiciary on H.R. 4709*, H.Rept. 109-395 (2006).

109-398) on March 16, 2006.[48] H.R. 4943 would prohibit deceitfully obtaining or selling the personal information of telecommunications customers, including customers' phone records. The bill provides an exemption from its prohibitions for any action by a law enforcement agency in connection with the performance of the official duties of the agency. The bill also would require telecommunications carriers to take precautions to safeguard customers' personal information and to notify customers and the Federal Communications Commission (FCC) whenever there is a breach in the security of this information. The FCC and the Federal Trade Commission (FTC) would enforce these restrictions and requirements. The bill also would direct the FCC to write regulations regarding security precautions for carriers, to periodically audit the security practices of telecommunication carriers, and to prepare reports on the assessment of the new regulations and requirements. It would increase the penalty for privacy violations to a minimum of $300,000 and a maximum of $3 million. Under current law, the penalty ranges from $100,000 to $1 million.

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). S. 2178 was reported by the Senate Judiciary Committee without report on March 2. This bill 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, and to prohibit the sale of such records by any person, including any employee of a covered entity. The bill exempts law enforcement agencies. It imposes a fine and/or imprisonment for up to five years, and doubles such penalties for violations occurring in a 12-month period involving more than $100,000 or more than 50 customers of a covered entity.

S. 2264, Consumer Phone Record Security Act of 2006 (Pryor) prohibits the unauthorized access or use of customer proprietary network information, the unauthorized sale of customer proprietary network information, and solicitation to obtain customer proprietary network information. The bill makes an exception for law enforcement agencies that seek to obtain telephone records in connection with official law enforcement duties. A violation would be treated as a violation of the Federal Trade Commission Act. Concurrent enforcement by the Federal Communications Commission is also provided for. A State may bring a civil action on behalf of its residents in an appropriate district court of the United States to enforce the prohibitions or to impose the authorized civil penalties. An individual whose customer proprietary network information has been obtained, used, or sold

---

[48] *Prevention of Fraudulent Access to Phone Records Act: Report of the House Committee on Energy and Commerce on S. 4963*, H.Rept. No. 109-398 (2006).

may bring a civil action in any court of competent jurisdiction against the person, excluding a telecommunications carrier, who committed the violation seeking a civil penalty of not more than $11,000 for each violation of this Act; and such additional relief as the court deems appropriate, including the award of court costs, investigative costs, and reasonable attorney's fees. Telecommunications carriers are required to comply with additional provisions to protect customer proprietary network information.

S. 2389, Protecting Consumer Phone Records Act (Allen). S. 2389 was reported by the Senate Commerce, Science and Transportation Committee on March 30. The bill amends the Communications Act of 1934 to prohibit the unlawful acquisition and use of confidential customer proprietary network information. This bill prohibits the acquisition or use of customer proprietary network information (CPNI) without the affirmative written consent of the customer; misrepresentation of customer consent to the acquisition or use of CPNI; unauthorized access to system or records of a telecommunications carrier or an IP-enabled voice service provider to acquire CPNI; the sale of CPNI; or requests for another person to obtain CPNI in an unlawful manner. The bill authorizes a civil action in state court or federal district court by a telecommunications carrier or an IP-enabled voice service provider based on violations of its provisions or prescribed regulations to recover actual money damages, and/or $11,000 for each violation. Treble damages may be assessed by the court for willful and knowing violations. Violators are subject to civil penalties up to $11,000 per violation or each day of continuing violation up to $11,000,000. Subscribers are expressly not authorized to bring a civil action for violations of this Act of section 222 of the Communications Act of 1934. The Federal Communications Commission (FCC) is directed to issue regulations (similar to the Federal Trade Commission's Safeguards Rule for personal consumer information) within 180 days of enactment to require a telecommunications carrier or a IP-enabled voice service provider to ensure the security and confidentiality of CPNI, to protect CPNI against threats and hazards, and to protect CPNI from unauthorized access or use that could result in substantial harm or inconvenience to customers. Covered entities are required to annually certify to the FCC their compliance. Civil forfeiture penalties for each violation up to $30,000, or 3 times that amount for each day of continuing violation not to exceed $3,000,000 may be imposed. Criminal fines for willful and knowing violations may also be imposed. The FCC is required to promulgate regulations requiring covered entities to notify each customer, within 14 calendar days of any incident the covered entity becomes or is made aware that CPNI is improperly disclosed. The Federal Trade Commission has primary enforcement authority for this Act, and violations are to be treated as violations of the Federal Trade Commission Act. The FCC has concurrent jurisdiction. State Attorneys General may bring civil actions in federal district court after notifying the FTC and FCC which has the option of intervening. This bill preempts any state statute, regulation, or rule that requires covered entities to develop, implement, or maintain procedures for protecting CPNI, or that restricts or regulates a covered entities ability to use, disclose, or permit access to such information; and preempts any state law or court ruling that imposes liability on a carrier or provider for failure to comply with any statute, rule, or regulation describing in the preceding sentence or with this Act or with section 222 of the Communications Act or its regulations. The bill does not preempt state contract or tort law, or other state laws that relate to acts of fraud or

computer crime. The FTC and FCC are required to consumer outreach and education campaign about the protection of CPNI