Order Code RL34409

CRS Report for Congress

Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers

March 10, 2008

Kathleen Ann Ruane
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers

Summary

Telephone records contain a large amount of intimate personal information. Recent years have seen a rise in the use of this information for marketing and even for criminal purposes. The purchase and sale of telephone record information, therefore, became a booming business. Websites and data brokers claiming to be able to obtain the phone records for any phone number within a few days abounded. However, the methods by which these data brokers obtained their information came under intense fire from public interest groups concerned about consumer privacy.

Consumer groups and news outlets reported that telephone records were being obtained fraudulently by data brokers or other individuals without the knowledge or consent of the customers to whom the records related. 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.

In response to increased concern over the unauthorized disclosure of private telephone records, Congress and other regulatory agencies have taken a number of steps to improve the security of this information. Congress enacted the Telephone Records and Privacy Protection Act of 2006, which makes "pretexting" a federal offense. The Federal Trade Commission has instituted a number of enforcement actions against data brokers. In the 110th Congress, bills have been introduced to ensure greater security of phone records. And the FCC recently amended its regulations governing the disclosure of Customer Proprietary Network Information (CPNI) in an attempt to address the concerns raised by Congress, the Electronic Privacy Information Center (EPIC), and other consumer groups regarding the unauthorized disclosure of such information.

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 laws that address disclosure of telephone records to the government, see CRS Report RL33424, *Government Access to Phone Calling Activity and Related Records*, by Elizabeth B. Bazan, Gina Marie Stevens, and Brian Yeh. 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*, by Gina Marie Stevens and Charles Doyle. This report will be updated when warranted.

Contents

Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers

Background[1]

In response to a petition filed by the Electronic Privacy Information Center (EPIC) concerning numerous websites advertising the sale of personal telephone records, the Federal Communications Commission conducted a rulemaking to determine the extent of the problem and construct regulations in response to consumer concerns.[2] Specifically, EPIC and other commenters pointed out that 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 claimed to provide calling records for landline and Voice over Internet Protocol (VOIP) phones, as well as nonpublished phone numbers. Data brokers claimed 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.[3] 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 had 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.

---

[1] The previous version of this report is available as an archived product. CRS Report RL33287, *Data Security: Protecting the Privacy of Phone Records*, by Gina Marie Stevens, Legislative Attorney.

[2] 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/].

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

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, made it easier for someone to impersonate the account holder to convince the employee that they were the account holder. For this reason, it was suggested that phone companies cease the use of readily available biographical information, like the Social Security number, for identity authentication.

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.

In response to these concerns, Congress, the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) have acted to prevent the unauthorized disclosure of phone records. The federal government has moved to directly address the problem of "pretexting" and to more clearly define the protective framework that telecommunications carriers must implement.

Federal Laws

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 RL34120, *Information Security and Data Breach Notification Safeguards*, by Gina Marie Stevens.

Pretext calling for financial information has long been illegal.[4] In 2006, Congress enacted the Telephone Records and Privacy Protection Act, which makes pretexting for the acquisition of telephone records a federal offense. Furthermore, several other federal statutes address illegal conduct associated with identity theft and pretext calling.[5]

Telephone Records and Privacy Protection Act. Section 3 of the act makes it a crime to knowingly and intentionally obtain, or attempt to obtain, "confidential phone records information"[6] of a covered entity (defined as a

---

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

[5] 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].

[6] "The term 'confidential phone records information' means information that — (A) relates

(continued...)

telecommunications carrier or an IP-enabled voice service provider) by making false statements or representations to an employee of a covered entity, making false or fraudulent statements to a customer of a covered entity, providing a document to a covered entity knowing that the document is false or fraudulent, or accessing customer accounts via the Internet without prior authorization from the customer to whom the information pertains.[7] The act further makes it a crime, except as otherwise provided by law or regulation, to knowingly and intentionally purchase, receive, transfer, or sell these records if they were obtained without the consent of the customer to whom the records relate.[8] This act is not applicable to law enforcement agencies.[9]

Penalties. For a violation of Section 3, an individual may be fined not more than $250,000, imprisoned for not more than 10 years, or both.[10] Violations of this section of the act by organizations may result in fines up to $500,000.[11] The act also provides for enhanced penalties for violations in certain situations. First, whoever violates Section 3 of the act, as described above, "while violating another law of the United States or as part of a pattern of any illegal activity involving more than $100,000, or more than 50 customers of a covered entity, in a 12-month period shall," in addition to penalties already provided for, be fined $500,000 in the case of an individual's violation or $1,000,000 in the case of an organization's violation (as the case may be), "imprisoned for not more than five years, or both."[12] Second, whoever violates Section 3 of the act, as described above, "in furtherance of, or with the intent to commit" the offenses of interstate domestic violence, stalking, interstate violation of a protective order, or any other crime of violence, in addition to penalties already provided for in the act, shall be fined and imprisoned for not more than five years.[13] Third, whenever an individual violates Section 3 of the act, as described above, "in furtherance of, or with the intent to commit" certain crimes against federal, state or local law enforcement or "to intimidate, threaten, harass, injure, or kill any Federal, State, or local law enforcement officer," the act provides that in

---

[6] (...continued)
to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; (B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer." P.L. 109-476; 18 U.S.C. § 1309(h)(1).

[7] P.L. 109-476; 18 U.S.C. §1039(a).

[8] P.L. 109-476; 18 U.S.C. §1039(b)-(c).

[9] P.L. 109-476, 18 U.S.C. § 1039(g).

[10] P.L. 109-476; 18 U.S.C. § 1039; 18 U.S.C. § 3571(b)(3). The act also provides for enhanced penalties under certain circumstances. 18 U.S.C. § 1039(d)-(e).

[11] 18 U.S.C. § 3571(c)(3).

[12] P.L. 109-476; 18 U.S.C. § 1039(d).

[13] P.L. 109-476; 18 U.S.C. § 1039(e)(1).

addition to the penalties already provided, that individual shall also be assessed an additional fine and imprisoned not more than five years.[14]

Federal Trade Commission Act. The FTC may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices.[15] 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 May 2006, the Federal Trade Commission 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, which prohibits unfair or deceptive acts or practices in or affecting commerce.[16] The agency sought 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.[17] In four of the five cases, the FTC succeeded in permanently enjoining the sale of phone records as well as imposing monetary penalties on the perpetrators.[18]

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.[19] Section 222 attempts to achieve a balance between marketing and customer privacy.

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

---

[14] P.L. 109-476; 18 U.S.C. § 1039(e)(2).

[15] 15 U.S.C. §§ 41-58.

[16] 15 U.S.C. § 45(a).

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

[18] Telephone Records Seller Settles FTC Charges, October 5, 2006, at [http://www.ftc.gov/opa/2006/10/isis.shtm]; Telephone Records Seller Settles FTC Charges, March 9, 2007, at [http://www.ftc.gov/opa/2007/03/infosearch.shtm]; Telephone Records Seller Settles FTC Charges, December 17, 2007, at [http://www.ftc.gov/opa/2007/12/ceo.shtm]; District Court Bars the Sale of Consumers' Telephone Records to Third Parties, January 28, 2008, at [http://www.ftc.gov/opa/2008/01/telrec.shtm].

[19] 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.)

> (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.[20]

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.[21] 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.[22]

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 provision of such telecommunications service, including the publishing of directories.[23]

---

[20] 47 U.S.C. § 222(h)(1).

[21] 47 U.S.C.§ 222(a).

[22] 47 U.S.C. § 222(b).

[23] 47 U.S.C. § 222(c)(1).

A carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[24] 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).[25] 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.[26]

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.[27]

Customer Proprietary Network Information (CPNI) Regulations. In 1998, the Federal Communications Commission issued its CPNI Order to implement Section 222.[28] 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 to market services outside of the customer's relationship with the carrier. The United

---

[24] 47 U.S.C. § 222(c)(2).

[25] 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).

[26] 47 U.S.C. § 222(d).

[27] 47 U.S.C. § 222(e).

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

States Court of Appeals for the Tenth Circuit struck down those rules, finding that they violated the First and Fifth Amendments of the Constitution.[29]

In response to the Tenth Circuit's remand, the FCC amended its CPNI regulations to require telecommunications carriers to receive opt-in (affirmative) consent before disclosing CPNI to third parties or affiliates that do not provide communications-related services.[30] However, carriers were permitted to disclose CPNI to affiliated parties, joint venture partners, and independent contractors after obtaining a customer's "opt-out" consent. "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.)[31]

On April 2, 2007, the FCC issued an order amending its Customer Proprietary Network Information Regulations and largely accepting EPIC's proposed changes.[32] The revised rules broaden the opt-in requirement for sharing CPNI with third parties and affiliated entities that do not provide a telecommunications service[33] to include joint venture partners and independent contractors as well.[34] Opt-out consent remains acceptable for sharing CPNI with affiliates that provide telecommunications services.[35] Carriers are required, prior to soliciting the customer's approval, to provide notice of the customer's right to restrict use, disclosure, and access to the customer's CPNI.[36]

Carriers are also required to establish safeguards to protect against the unauthorized disclosure of CPNI. To that end, carriers must maintain records that track access to customer CPNI records.[37] The FCC also has implemented carrier authentication requirements for the disclosure of call detail information under which carriers are not allowed to release call detail information during a customer-initiated

---

[29] *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).

[30] 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)-(c), 64.2007(b); 64.2008(e); see also 47 C.F.R. § 64.2003(h) (defining "opt-in approval").

[31] 47 C.F.R. § 64.2003(l).

[32] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, 22 FCC Rcd 6927 (2007).

[33] 47 C.F.R. §§ 64.2005(b)-(c), 64.2007(b).

[34] *Id.*

[35] 47 C.F.R. § 64.2005(a).

[36] 47 C.F.R. § 64.2008.

[37] 47 C.F.R. § 64.2009.

phone call, except when the customer provides a pre-established password.[38] If the customer does not or cannot provide the password, the carrier may release the call detail information only by sending the information to the address of record for the account or through backup authentication methods that do not use readily available biographical information (such as a social security number, or mother's maiden name).[39] Carriers also must establish passwords for online account access.[40] Carriers must provide notice to customers whenever changes to their accounts occur, as well as adhere to a notification process for both law enforcement and affected customers in the event of unauthorized or improper disclosure of CPNI.[41]

Each carrier is also required to certify annually its compliance with the CPNI regulations and to make this certification publicly available.[42] The certification must contain a list of customer complaints regarding unauthorized disclosure of CPNI for the previous year. It is worth noting that the FCC's most recent order extended its CPNI regulations to cover interconnected Voice-Over-Internet-Protocol (VOIP) service providers.[43]

Penalties. 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 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.[44]

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

---

[38] 47 C.F.R. § 64.2010(b).

[39] 47 C.F.R. § 64.2010(b),(e).

[40] 47 C.F.R. § 64.2010(c).

[41] 47 C.F.R. §§ 64.2010(f), 64.2011.

[42] 47 C.F.R. §§ 64.2009(e).

[43] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, 22 FCC Rcd 6927 at ¶ 54.

[44] 47 U.S.C. § 502.

the United States for a civil money "forfeiture" penalty.[45] 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.[46] 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.

Litigation

The National Cable and Telecommunications Association (NCTA) has challenged the FCC's new requirement for carriers to obtain opt-in consent for sharing CPNI with joint venture partners and independent contractors in the U.S. Court of Appeals for the DC Circuit.[47] NCTA argues that the new opt-in rule is arbitrary and capricious and that it violates the First Amendment rights of carriers. NCTA does not challenge the remainder of the recently implemented rules. The case is currently in its preliminary stages.

Congressional Response

Legislation has been introduced in the 110th Congress to address the problems presented by unauthorized disclosure of telephone records. Generally, the bills would expand the enforcement authority of the FTC to punish pretexting and unauthorized receipt of confidential customer information and would require the FCC to ensure that telecommunications carriers and IP-enabled voice service providers are taking proper care to safeguard the privacy of these records. Many of the substantive requirements for regulatory action contained in the proposed legislation were implemented by the FCC's most recent rulemaking. None of the bills has been reported out of committee.

H.R. 852, Consumer Telephone Records Protection Act of 2007 (Inslee). H.R. 852 is similar in substance to the Telephone Records and Privacy Protection Act of 2006 in that it prohibits obtaining or attempting to obtain confidential phone records by fraud or false statement and prohibits the purchase or sale of such fraudulently obtained information. The bill also would amend Section

---

[45] 47 U.S.C. § 503(b)(1).

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

[47] Petition for Review, National Cable & Telecommunications Association v. Federal Communications Commission, U.S. Court of Appeals for the DC Circuit (August 7, 2007), available at [http://www.ncta.com/PublicationType/JudicialFiling/4323.aspx].

222 of the Communications Act of 1934 to direct the FCC to promulgate regulations that would require telecommunications carriers to notify customers when CPNI has been disclosed improperly, and grants enforcement authority to the FTC.

H.R. 936, Prevention of Fraudulent Access to Phone Records Act (Dingell). H.R. 936 grants the FTC specific authority to enforce its prohibition on the fraudulent acquisition of customer proprietary network information as it would a violation of a rule defining an unfair or deceptive act or practice prescribed by the FTC act. Furthermore, the bill would expand the protections of detailed customer records maintained by telecommunications carriers by prohibiting disclosure of CPNI by telecommunications carriers to joint venture partners, independent contractors, or any other third parties except with the express prior authorization of the customer. The bill also would direct the FCC to promulgate regulations that would require telecommunications carriers, for example, to notify customers of unauthorized disclosures of CPNI, to maintain records of each time CPNI is requested or accessed, and to establish a security policy to ensure the confidentiality of CPNI.

S. 92 (Stevens) and S. 780 (Pryor), Protecting Consumer Phone Records Act. Except as authorized by other law or regulation, S. 92 and S. 780 would make it unlawful to obtain, transfer, sell, or purchase CPNI without the express written consent of the customer to whom the CPNI relates. These proposals would create a private right of action against violators of the act for telecommunications carriers (as well as IP-enabled voice service providers) and for consumers with the possible award of treble damages if the court finds a knowing and willful violation. The bills would further require the FCC to revise its CPNI regulations to increase the security and confidentiality of CPNI. Concurrent enforcement jurisdiction would be granted to the FCC and the FTC for violations of the act.