Order Code RL33424

CRS Report for Congress

Government Access to Phone Calling Activity and Related Records: Legal Authorities

Updated January 25, 2007

Elizabeth B. Bazan, Gina Marie Stevens, and Brian T. Yeh
Legislative Attorneys
American Law Division

Prepared for Members and
Committees of Congress

Government Access to Phone Calling Activity and Related Records: Legal Authorities

Summary

Media disclosures regarding an alleged National Security Agency (NSA) program designed to collect and analyze information on telephone calling patterns within the United States have raised interest in the means by which the Government may collect such information. The factual information available in the public domain with respect to any such alleged program is limited and in some instances inconsistent, and the application, if at all, of any possibly relevant statutory provisions to any such program is likely to be a very fact specific inquiry. It is possible that any information provided to the NSA from the telephone service providers was provided in response to a request for information, not founded on a statutory basis. If this were the case, such a request would not necessarily be limited by the statutory structures discussed below, but in some instances, depending upon the facts involved, might expose the telephone companies to some civil remedies or criminal sanctions. In addition, a request, not founded upon a statutory scheme, would appear to lack a means of compelling production of the information requested. This would seem to be consistent with the statement in the *USA Today* article of May 11, 2006, that one of the companies refused to comply with NSA's request for calling detail records, while at least one other company appears to have complied.

Numerous lawsuits have been filed by civil liberties groups against several telecommunications companies on behalf of their customers and subscribers, for their alleged cooperation with the NSA program that have harmed the plaintiffs' constitutional and statutory rights. One case, *Hepting v. AT&T Corp.*, was filed in January 2006 and is based in part on evidence of participation in the NSA program by the defendant provided by a former AT&T employee, whereas all the other lawsuits were filed after the publication of the *USA Today* article and are based largely on the factual allegations made therein. On August 9, 2006, the Federal Judicial Panel on Multidistrict Litigation transferred 17 cases, with 26 additional cases treated as potential tag-along actions, that are pending throughout the country to the Northern District of California, and assigned them to U.S. District Judge Vaughn R. Walker for coordinated or consolidated pretrial proceedings, *In Re: National Security Agency Telecommunications Records Litigation*, MDL-1791. As of January 10, 2007, 42 actions were consolidated in the multidistrict litigation and are still ongoing.

This report summarizes statutory authorities regarding access by the government, for either foreign intelligence or law enforcement purposes, to information related to telephone calling patterns or practices. Where pertinent, it also discusses statutory prohibitions against accessing or disclosing such information, along with relevant exceptions to those prohibitions.

Contents

Government Access to Phone Calling Activity and Related Records: Legal Authorities

Introduction

Media disclosures regarding an alleged National Security Agency (NSA) program designed to collect and analyze information on telephone calling patterns within the United States have raised interest in the means by which the Government may collect such information. According to the information in the *USA Today* news story from May 11, 2006, the NSA is alleged to have sought and obtained records of telephone numbers called and received from millions of telephones within the United States from three telephone service providers, while a fourth had refused to provide such records.[1] Several days after the publication of that news article, two of the three service providers originally reported to have provided calling records denied that they provided such records.[2] The *USA Toda*y article indicated that no names or addresses were obtained in connection with these telephone calls, nor were the contents of these telephone calls sought or obtained. The *USA Today* story also stated that one telephone service provider had refused to provide the NSA access to such information because of concerns about the legality of such disclosures. The *USA Today* story indicated that this information was being compiled in a database and being used for pattern analysis. The President, in his weekly radio address on May 13, 2006, while discussing his nomination of General Michael V. Hayden to head the Central Intelligence Agency, has responded to the news reports of NSA's alleged data mining activities:

> This week, new claims have been made about other ways we are tracking down al Qaeda to prevent attacks on America. It is important for Americans to understand that our activities strictly target al Qaeda and its known affiliates. Al Qaeda is our enemy, and we want to know their plans. The intelligence activities I have authorized are lawful and have been briefed to appropriate members of Congress, both Republican and Democrat. The privacy of all Americans is

---

[1] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls; 3 Telecoms Help Government Collect Billions of Domestic Records*, USA TODAY, May 11, 2006, at 1A. The story alleged that Verizon, BellSouth, and AT&T provided calling records in response to the NSA's inquiry or production demand, while Qwest did not.

[2] In a "note" to its readers on June 30, 2006, USA Today issued a partial retraction of its original story, stating that it "has now concluded that while the NSA has built a massive domestic calls record database involving the domestic call records of telecommunications companies, the newspaper cannot confirm that BellSouth or Verizon contracted with the NSA to provide bulk calling records to that database." *A Note To Our Readers*, USA TODAY, June 30, 2006, at 2A.

> fiercely protected in all our activities. The government does not listen to domestic phone calls without court approval. We are not trolling through the personal lives of millions of innocent Americans. Our efforts are focused on links to al Qaeda terrorists and its affiliates who want to harm the American people.
>
> Americans expect their government to do everything in its power under our laws and Constitution to protect them and their civil liberties. That is exactly what we are doing. And so far, we have been successful in preventing another attack on our soil....

The factual information available in the public domain with respect to any such alleged program is limited and in some instances inconsistent, and the application, if at all, of any possibly relevant statutory provisions to any such program is likely to be a very fact specific inquiry. It is possible that any information provided to the NSA from the telephone service providers was provided in response to a request for information, not founded on a statutory basis. If this were the case, such a request would not necessarily be limited by the statutory structures discussed below, but in some instances, depending upon the facts involved, might expose the telephone companies to some civil remedies or criminal sanctions. In addition, a request, not founded upon a statutory scheme, would appear to lack a means of compelling production of the information requested. This would seem to be consistent with the statement in the *USA Today* article that one of the companies refused to comply with NSA's request for calling detail records, while at least one other company appears to have complied.

Numerous lawsuits have been filed by civil liberties groups against telecommunications companies on behalf of their customers and subscribers, for their alleged cooperation with the NSA program that have harmed the plaintiffs' constitutional and statutory rights. *Hepting v. AT&T Corp.*[3] was filed in January 2006 and is based in part on evidence of participation by the defendant in the NSA program provided by a former AT&T employee, whereas all the other lawsuits were filed after the publication of the *USA Today* article and are based largely on the factual allegations made therein. On May 13, 2006, the government moved to intervene as a defendant in the *Hepting* case and moved to dismiss the action or, in the alternative, for summary judgment in favor of AT&T, based on the "state secrets" privilege, a common law evidentiary rule that protects information from civil discovery when disclosure would harm national security. U.S. District Judge Vaughn R. Walker allowed the *Hepting* case to proceed by rejecting the government's state secrets claim because of the public disclosures about the litigation's subject matter by AT&T and the government.[4] The judge also denied AT&T's motion to dismiss the case on the basis of its claim of qualified immunity from liability for assisting the government. On November 7, 2006, the U.S. Court of Appeals for the Ninth Circuit granted the defendants' petition for interlocutory review of Judge Walker's ruling,[5] but has not yet reached a decision on the appeal as of January 2007. Judge Walker

---

[3] No. C:06-cv-0672-VRW (N.D. Cal. 2006),

[4] Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 994 (N.D. Cal. July 20, 2006).

[5] Hepting v. United States, Nos. 06-80109, 06-80110 (9th Cir. 2006) (order granting appeal).

has scheduled a February 9, 2007, hearing to consider the government's motion to enter a stay in the proceedings pending resolution of the Ninth Circuit's review of his order.

On August 9, 2006, pursuant to 28 U.S.C. § 1407, the Judicial Panel on Multidistrict Litigation transferred 17 civil actions that were pending throughout the country, including *Hepting*, to the Northern District of California, and assigned them to Judge Walker for coordinated or consolidated pretrial proceedings. Another 26 cases were treated as potential tag-along actions under the multidistrict litigation rules.[6] The panel of five federal trial and appellate court judges found that all these class actions share "factual and legal questions regarding alleged Government surveillance of telecommunications activity and the participation in (or cooperation with) that surveillance by individual telecommunications companies," and thus centralization of the cases "is necessary in order to eliminate duplicative discovery, prevent inconsistent pretrial rulings (particularly with respect to matters involving national security), and conserve the resources of the parties, their counsel and the judiciary."[7] As of January 10, 2007, 42 actions had been included in this consolidated case. The February 9, 2007, hearing mentioned above will also address whether Judge Walker's *Hepting* order should apply to all cases and claims to which the Government asserts the state secrets privilege.

This report summarizes statutory authorities regarding access by the Government, for either foreign intelligence or law enforcement purposes, to information related to telephone calling patterns or practices. Where pertinent, it also discusses statutory prohibitions against accessing or disclosing such information, along with relevant exceptions to those prohibitions.

Background

The Supreme Court, in *Smith v. Maryland*, 442 U.S. 735 (1979), in a pen register case, has held that there is no Fourth Amendment protected reasonable expectation of privacy in records of telephone calls in the hands of third party providers, where contents of those calls is not intercepted. The Fourth Amendment to the United States Constitution guarantees:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation,

---

[6] Rule 1.1 of the Rules of Procedure for Multidistrict Litigation defines a "tag-along action" as referring "to a civil action pending in a district court and involving common questions of fact with actions previously transferred" under 28 U.S.C. § 1407.

[7] Transfer Order, MDL Docket No. 1791, *In Re: National Security Agency Telecommunications Records Litigation*, *available at* [http://www.jpml.uscourts.gov/MDL-1791-TransferOrder.pdf].

> and particularly describing the place to be searched, and the persons or things to be seized.[8]

Whether the use of a pen register is a "search and seizure" within the meaning of the Fourth Amendment determines if the government, in compliance with the Constitution, must secure a warrant or court order prior to its installation. In 1979, the United States Supreme Court decided this question in *Smith v. Maryland*,[9] holding that the Fourth Amendment does not prohibit the use of pen registers without a warrant. Writing the majority opinion joined by four other justices, Justice Harry Blackmun drew a distinction between the acquisition of contents of telephone communications using electronic listening devices, which the Court in *Katz v. United States*[10] had deemed to be a "search" under the Fourth Amendment, and the capture of electronic impulses that identify the numbers dialed on a telephone using a pen register device. According to the majority in *Smith*, it is a constitutionally significant difference that pen registers do not record the *contents* of communications, in contrast to the listening devices employed in *Katz*.[11] The Court explained that the Fourth Amendment does not apply to the use of pen registers because individuals do not have a legitimate expectation of privacy against invasion by government action, concerning the numbers dialed into a telephone system:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law."[12]

The Court stated that telephone customers, by voluntarily conveying phone numbers to the telephone company and "expos[ing] that information to its equipment in the ordinary course of business," assume the risk that the company may disclose such information to law enforcement.[13] Because there is no actual or legitimate expectation of privacy in the numbers dialed from a telephone, the installation and use of a pen register is not a "search" requiring a warrant under the Fourth Amendment, the Court ruled.[14]

The dissenting opinions in *Smith* believed that telephone numbers dialed from a phone are entitled to the same constitutional protection that telephone conversations receive under *Katz* because such numbers are not without "content" - they "reveal the

---

[8] U.S. CONST. amend. IV.

[9] 442 U.S. 735 (1979).

[10] 389 U.S. 347 (1967).

[11] *Smith*, 442 U.S. at 741 (emphasis in original).

[12] *Id.* at 742 (quoting United States v. New York Tel. Co., 434 U.S. 159, 174-75 (1977)).

[13] *Id.* at 744.

[14] *Id.* at 745-46.

identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[15] Furthermore, the dissenters objected to the majority's characterization that the use of a telephone involves an assumption of risk on the part of the customer that telephone dialing information might be disclosed to the government; assumption of risk generally requires there to have been a choice to engage in the activity, and "as a practical matter, individuals have no realistic alternative" to the use of a telephone.[16]

There are, however, a number of statutes enacted since 1979, which both permit access by the Government, for foreign intelligence or law enforcement purposes, to information relating to telephone numbers dialed from or received by a particular telephone number, as well as duration and usage, and which impose limitations as to how such information may be accessed and under what circumstances it may be used. Some of these statutes also provide criminal penalties for violations of their provisions and provide civil remedies to those adversely impacted by such violations. In addition, the Communications Act of 1934, as amended, addresses protections to customer proprietary network information, and provides civil and criminal penalties for violations of its provisions or implementing regulations.

Statutory Provisions

Summary

Information regarding telephone calling patterns, duration, usage, and length of service may be sought by the government either directly through the use of pen registers[17] or trap and trace devices,[18] or indirectly by seeking telephone toll or transactional records from third party providers. Statutory provisions authorizing,

---

[15] *Id.* at 747-48 (Stewart, J., dissenting).

[16] *Id.* at 749 (Marshall, J., dissenting).

[17] Under 50 U.S.C. § 1841(2), which cross references the definition in 18 U.S.C. § 3127(3), the term "pen register" "means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."

[18] Under 50 U.S.C. § 1841(2), which cross references the definition in 18 U.S.C. § 3127(4), the term "trap and trace device" "means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

pursuant to court order, the use of pen registers and trap and trace devices exist in both the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1841 *et seq*., and, for law enforcement purposes, in 18 U.S.C. § 3121 *et seq*.

FISA's "business records" provision, 50 U.S.C. § 1861, provides for authority, pursuant to court order, for requests for production of "any tangible thing" relevant to collection of foreign intelligence information not concerning a U.S. person, or relevant to an investigation into international terrorism or clandestine intelligence activities. Under 50 U.S.C. § 1861, an investigation concerning a U.S. person may not be based solely on First Amendment protected activities.

Access to stored electronic communications is addressed in 18 U.S.C. § 2701 *et seq*. 18 U.S.C. § 2702 prohibits voluntary disclosure of customer communications records by a service provider unless it falls within one of several exceptions. Required disclosure of customer records to the government under certain circumstances is addressed under 18 U.S.C. § 2703, including, among others, disclosure pursuant to a warrant or grand jury or trial subpoena. 18 U.S.C. § 2709 is a national security letter provision, under which a wire or electronic service provider[19] must provide subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession in response to a request by the Director of the Federal Bureau of Investigation (FBI) if the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge designated by the FBI Director in a field office, certifies that the records or information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of First Amendment protected activities. In addition, Section 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222, provides protections to customer proprietary network information, and violations of pertinent provisions of law or regulation may expose service providers to criminal provisions, civil penalties and forfeiture provisions, 47 U.S.C. §§ 501-503. There follows a more detailed description of these provisions.

---

[19] Under 18 U.S.C. § 2709(f), "A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title." Subsection (f) was added by P.L. 109-178, § 5.

50 U.S.C. § 1842 — Pen Registers and Trap and Trace Devices for Foreign Intelligence and International Terrorism Investigations Under FISA

Under this provision,[20] the Attorney General or a designated attorney for the Government may apply for an ex parte court order authorizing the use of a pen register or trap and trace device to a Foreign Intelligence Surveillance Court (FISC) judge or to a U.S. magistrate judge designated by the Chief Justice of the United States to have the power to hear applications or grant orders approving installation and use of a pen register or trap and trace device on behalf of an FISC judge. The application must be approved by the Attorney General or a designated Government attorney; must identify the Federal officer seeking to use the pen register or trap and trace device; and must include a certification that the information likely to be obtained is foreign intelligence information[21] not concerning a U.S. person[22] or that the information is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. An investigation of a U.S. person may not be conducted solely on the basis of First Amendment protected activities.

The order must specify the identity of the person who is the subject of the investigation, if known. If known, the order must identify the person to whom the telephone line or other facility to which the pen register or trap and trace device is to be attached is leased or in whose name it is listed. In addition, the order must list the attributes of the communications to which it applies, such as the number or other identifier and, if known, the location of the telephone line or other facility involved. In the case of a trap and trace device, the order must also identify the geographic limits of the trap and trace order.

---

[20] Other provisions of this chapter deal with authorization for pen registers or trap and trace devices during emergencies, 50 U.S.C. § 1843, authorization during time of war, 50 U.S.C. 1844, use of information gathered under a FISA pen register or trap and trace device, 50 U.S.C. § 1845, and congressional oversight, 50 U.S.C. § 1846.

[21] Under 18 U.S.C. § 1801(e), "foreign intelligence information" is defined to mean information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, sabotage or international terrorism by a foreign power or an agent of a foreign power, or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the national defense or the security of the United States or the conduct of the foreign affairs of the United States.

[22] Under 50 U.S.C. § 1801(i), "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Such an order, at the request of the applicant, also directs the provider of the wire or electronic service, landlord, custodian, or other person, to furnish any information, facilities, or technical assistance needed to accomplish the installation and operation of the pen register or trap and trace device in a manner that will protect its secrecy and minimize interference with the services provided. In addition, the order directs the provider, landlord, custodian, or other person not to disclose the existence of the investigation or the pen register or trap and trace device to anyone unless or until ordered to do so by the court. Records concerning the pen register or trap and trace device or the aid furnished are to be kept under security procedures approved by the Attorney General and the Director of National Security under 50 U.S.C. § 1805(b)(2)(C).

The order also directs the applicant for the order to provide compensation for reasonable expenses incurred by the provider, landlord, custodian or other person in providing information, facilities, or technical assistance.

Upon the request of the applicant for the court order, the court shall direct the wire or electronic service provider to provide the federal officer using the pen register or trap and trace device with the name; address; and the telephone number, instrument number or subscriber number or identifier of the customer or subscriber using the service covered by the order for the period specified by the order, including temporarily assigned network address or associated routing or transmission information. The service provider must also provide, if so ordered by the court upon the applicant's request, information on length of service of the customer or subscriber, as well as local or long distance telephone records of the subscriber or customer, and, if applicable, any records on periods of usage by the customer or subscriber. Further, the court, at the applicant's request, may order disclosure by the service provider of any mechanisms and sources of payment for the service (i.e., credit card, bank account).

If the information is available with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order, the court, upon the request of the applicant for the order, is to direct the wire or electronic service provider to provide the name; address; telephone number, instrument number or other subscriber number or identifier, of such customer or subscriber, as well as length of service provided to and types of serviced utilized by the subscriber or customer.

In general, the duration of an order issued under this section is not to exceed 90 days, with the possibility of extension for periods of not more than 90 days. However, if the applicant for the order certifies that the information likely to be obtained is foreign intelligence information not concerning a United States person, then an extension may be for up to a year. No cause of action may be brought against any wire or electronic service provider, landlord, custodian, or other person that furnishes information, facilities, or technical assistance pursuant to an order issued under this provision. Unless otherwise ordered by the judge, the results of the pen register or trap and trace device are to be provided to the authorized Government official or officials at reasonable intervals.

18 U.S.C. § 3121-3123 — Pen Registers or Trap and Trace Devices Generally, and for Use in an Ongoing Criminal Investigation

18 U.S.C. § 3121 prohibits the installation and use of a pen register or trap and trace device without first obtaining a court order under FISA or under 18 U.S.C. § 3123. This prohibition does not apply to use by an electronic or wire service provider relating to the operation, maintenance and testing of a service or protection of the rights or property of the service provider; the protection of users of the service from abuse or unlawful use of the service; to recording of the fact that a wire or electronic communication was initiated or completed to protect the service provider, another provider furnishing service toward completion of the wire communication, or a user of the service from fraudulent, unlawful or abusive use of the service; or to use where the consent of the user of the service has been obtained. A government agency authorized to install and use a pen register or trap and trace device under the provisions of this chapter of Title 18, U.S.C., or under state law must use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications in a manner that does not include the contents of that communication.

An application for a court order authorizing a pen register or trap and trace device under this chapter must be made pursuant to 18 U.S.C. § 3122 in writing under oath or affirmation to a court of competent jurisdiction. Such an application must include the identity of the attorney for the Government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation, as well as a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. Under 18 U.S.C. § 3123, the court shall enter an ex parte order authorization installation and use of a pen register or trap and trace device anywhere in the United States if the court finds that the applicant for the order has made such a certification. An order may authorize installation and use of a pen register or trap and trace device for a period of up to 60 days, which can be extended by court order for additional periods of no more than 60 days. The order must also direct that the order be sealed until otherwise ordered by the court, and must prohibit the person owning or leasing the line or other facility to which the pen register or trap and trace device is attached or applied, or who is obligated by the order to assist the applicant, from disclosing the existence of the pen register or trap and trace device or of the investigation to the listed subscriber or to any other person unless or until the court orders otherwise.[23]

---

[23] 18 U.S.C. § 3124 addresses assistance in installation and use of the pen register or trap and trace device; while 18 U.S.C. § 3125 deals with emergency installation of a pen register and trap or trap and trace device. 18 U.S.C. § 2136 provides for annual reports to Congress by the Attorney General on the number of applications by law enforcement agencies of the Department of Justice for pen registers or trap and trace devices orders, as well as certain details with respect to court orders issued in response to such applications.

50 U.S.C. § 1861 — Access to Business Records for Foreign Intelligence and International Terrorism Investigations

Under 50 U.S.C. § 1861, the Director of the Federal Bureau of Investigation (FBI) or a designee of the Director, whose rank shall not be lower than Assistant Special Agent in Charge, may apply to the FISA court for an order granting the government access to any tangible item (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person, or to protect against international terrorism or clandestine intelligence activities. Such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the first amendment to the Constitution.

The application for such an order must include a statement of facts demonstrating that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized or preliminary investigation to protect against international terrorism or espionage, or to obtain foreign intelligence information not concerning a U.S. person.[24] However, certain tangible items are deemed presumptively relevant to an investigation if the application's statement of facts shows that the items sought pertain to a foreign power or an agent of a foreign power, the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.

The FISA court judge shall approve an application for an order under 50 U.S.C. § 1861, as requested or as modified, upon a finding that the application complies with statutory requirements. The order must contain a particularized description of the items sought, provide for a reasonable time to assemble them, and be limited to things which may be obtained under a grand jury subpoena or an order of a U.S. court for production of records or tangible things.[25] The order to produce the tangible things (production order) is also accompanied by a nondisclosure requirement (nondisclosure order) that prohibits the recipient from disclosing to any other person that the FBI has sought the tangible things described in the order, with limited exceptions.[26] The recipient may immediately challenge the legality of the production order by filing a petition with the FISA court; however, the recipient must wait one year before challenging the nondisclosure order.[27] A FISA court judge considering the recipient's petition to modify or set aside the production order may do so only if the judge finds that the order does not meet statutory requirements or is otherwise

---

[24] 50 U.S.C. § 1861(b)(2)(A).

[25] 50 U.S.C. § 1861(c).

[26] A recipient of a FISA order under this section may disclose its existence to persons to whom disclosure is necessary to comply with the order, to an attorney to obtain legal advice with respect to the production of things in response to the order, as well as to other persons approved by the FBI. 50 U.S.C. § 1861(d)(1).

[27] 50 U.S.C. § 1861(f)(2)(A).

unlawful.[28] A nondisclosure order may be modified or set aside if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person.[29] If, at the time the individual files the petition for judicial review of a nondisclosure order, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, then the FISA judge must treat such government certification as conclusive unless the judge finds that the certification was made in bad faith.[30]

18 U.S.C. § 2701 *et seq*. — Access to Stored Electronic Communications and Transactional Records

Access to stored electronic communications and transactional records is addressed in 18 U.S.C. § 2701 *et seq.* Under 18 U.S.C. § 2702, voluntary disclosure of customer communications records by a service provider is prohibited unless it falls within one of several exceptions, including, among others, disclosure as authorized in 18 U.S.C. § 2703; disclosure with the lawful consent of the customer or subscriber; or disclosure to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.[31] Under 18 U.S.C. § 2703, a provider of electronic communication service or remote computing service shall disclose to a government entity the name, address, local and long distance telephone connection records, or records of session times and durations, length of service and types of service utilized, telephone instrument number or other subscriber number or identity, including temporarily assigned network address, and means and source of payment for such service pursuant to: a warrant; a court order based upon specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication or the records or other information sought are relevant and material to an ongoing criminal investigation; customer or subscriber consent; or a written request from the governmental entity relevant to a law enforcement investigation regarding telemarketing fraud; or pursuant to an administrative subpoena authorized by federal or state statute, or a federal or state grand jury subpoena or trial subpoena. A governmental entity receiving such records or information is not required to provide notice to a subscriber or customer. Nor does any cause of action lie against any service provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for

---

[28] 50 U.S.C. § 1861(f)(2)(B).

[29] 50 U.S.C. § 1861(f)(2)(C)(i).

[30] 50 U.S.C. § 1861(f)(2)(C)(ii).

[31] This language was added by P.L. 109-177, Title I, § 107(b)(1)(B). It replaced an exception which covered "disclosure to a governmental entity if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."

providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization or certification under this chapter.

18 U.S.C. § 2706 requires a government entity obtaining records or other information under §§ 2702 or 2703 to reimburse the costs reasonably necessary and directly incurred in searching for, assembling, reproducing or otherwise providing such information. The amount of payment is to be mutually agreed upon by the government entity and the person or entity providing the information, or, in the absence of an agreement, determined by the court issuing the production order. The reimbursement requirement does not apply to records or other information maintained by a communications common carrier that relate to telephone records and telephone listings obtained under 18 U.S.C. § 2703 unless a court orders payment upon a determination that the information required is unusually voluminous in nature or otherwise caused an undue burden upon the provider.

Under 18 U.S.C. § 2709, a national security letter provision, wire or electronic service providers[32] must provide subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession in response to a request by the Director of the Federal Bureau of Investigation (FBI) if the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge designated by the FBI Director in a field office, certifies that the records or information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of First Amendment protected activities. Under 18 U.S.C. § 2709(b), if the Director of the Federal Bureau of Investigation, or his designee, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.[33] The FBI must notify

---

[32] Under 18 U.S.C. § 2709(f), "A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title." Subsection (f) was added by P.L. 109-178, § 5.

[33] P.L. 109-177, § 116(a), rewrote subsection (c) of 18 U.S.C. § 2709, which formerly read, "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section." P.L. 109-178, § 4(b), rewrote subsection (c)(4), as amended by P.L. 109-177, § 116(a), which formerly read, "At the request of the Director of the Federal Bureau of Investigation or the designee of the

(continued...)

the person or entity to whom a §2709(b) request is made where such a nondisclosure requirement is applicable. A recipient of such a request who notifies those to whom notice is necessary for compliance with the request or who notifies an attorney to obtain legal advice or legal assistance with respect to the request must also advise them of the nondisclosure requirement. At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request. The FBI may only disseminate records obtained under this section as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency. On a semiannual basis, the Director of the Federal Bureau of Investigation is required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Except as provided in 18 U.S.C. § 2703(e), 18 U.S.C. § 2707 provides a civil cause of action for any provider of electronic communication service, subscriber, or other person aggrieved by a knowing or intentional violation of this chapter. The aggrieved party may receive equitable relief and damages. The damages which may be assessed by the court are actual damages suffered by the plaintiff plus any profits made by the violator as a result of the violation. At a minimum, a person entitled to recover damages must receive no less than $1,000. If a court or appropriate department or agency determines that the United States has violated this chapter and that the circumstances surrounding the violation raise questions as to whether a federal officer or employee acted willfully or intentionally with respect to the violation, disciplinary action against that officer or employee may also be initiated.

A person aggrieved by a willful violation of this chapter or a willful violation of 50 U.S.C. § 1845(a), which deals use of information gathered through a pen register and trap and trace under FISA, may commence a civil action against the United States in a U.S. district court to receive money damages under 18 U.S.C. § 2712. If the claim is successful in establishing such a violation, the court may assess actual damages, but not less than $10,000, whichever is greater, plus reasonably incurred litigation costs. There is a two year statute of limitations applicable to this

---

[33] (...continued)
Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, but in no circumstance shall a person be required to inform the Director or such designee that the person intends to consult an attorney to obtain legal advice or legal assistance."

provision, and this section states that this is the exclusive remedy against the United States for claims within the purview of the section. The agency or department must reimburse any award under this section to the U.S. treasury. Administrative discipline may also be pursued. A proceeding under 18 U.S.C. § 2712 shall be stayed by the court, upon motion by the United States, if the court determines that civil discovery will adversely affect the Government's ability to conduct a related investigation or prosecution of a related criminal case. Such a stay would toll the statute of limitations.

47 U.S.C. §§ 222, 501-503 — Communications Act of 1934

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 its customers' customer proprietary network information.[34] 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

> (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.[35]

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.

---

[34] 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.).

[35] 47 U.S.C. § 222(h)(1).

Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information of other carriers, equipment manufacturers, and customers.[36] 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.[37]

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.[38]

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."[39] 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).[40] 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;[41] (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

---

[36] 47 U.S.C.§ 222(a).

[37] 47 U.S.C. § 222(b).

[38] 47 U.S.C. § 222(c)(1).

[39] 47 U.S.C. § 222(c)(2).

[40] 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).

[41] Whether the statutory provisions discussed in this report would fall within this exception is uncertain.

the call; and (4) provide call location information concerning the user of a commercial mobile service for emergency.[42]

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.[43]

Customer Proprietary Network Information (CPNI) Regulations. In 1998, the Federal Communications Commission issued its *CPNI Order* to implement section 222.[44] 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 States Court of Appeals for the Tenth Circuit struck down those rules, finding that they violated the First and Fifth Amendments of the Constitution.[45]

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.[46] However, carriers are permitted to disclose CPNI to affiliated parties after obtaining a customer's "opt-out" consent.[47] "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.)[48] 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

---

[42] 47 U.S.C. § 222(d).

[43] 47 U.S.C. § 222(e).

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

[45] *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).

[46] 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").

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

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

to the customer's CPNI.[49] 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.[50] Each carrier is also required to certify annually its compliance with the CPNI requirements and to make this certification publicly available.[51] The FCC recently proposed $100,000 fines on telephone companies with inadequate certifications regarding compliance with FCC rules protecting customer information from disclosure.[52]

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, 47 U.S.C. § 502, 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.[53]

Under section 503(b)(1) of the Act, 47 U.S.C. § 503(b)(1), 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.[54] Section 312(f)(1) of the Act, 47 U.S.C. § 312(f)(1), 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.[55] To impose such a forfeiture penalty, the Commission must issue

---

[49] 47 C.F.R. §§ 64.2008.

[50] 47 C.F.R. §§ 64.2009.

[51] 47 C.F.R. §§ 64.2009(e).

[52] 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].

[53] 47 U.S.C. § 502.

[54] 47 U.S.C. § 503(b)(1).

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

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.

[55] (...continued)
1.80(b).