



# Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

**Gina Stevens**

Legislative Attorney

**Charles Doyle**

Senior Specialist in American Public Law

October 9, 2012

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

98-327

**CRS Report for Congress**

*Prepared for Members and Committees of Congress*

## Summary

This report provides an overview of the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). ECPA consists of three parts. The first, often referred to as Title III, outlaws wiretapping and electronic eavesdropping, except as otherwise provided. The second, the Stored Communications Act, governs the privacy of, and government access to, the content of electronic communications and to related records. The third outlaws the use and installation of pen registers and of trap and trace devices, unless judicially approved for law enforcement or intelligence gathering purposes.

FISA consists of seven parts. The first, reminiscent of Title III, authorizes electronic surveillance in foreign intelligence investigations. The second authorizes physical searches in foreign intelligence cases. The third permits the use and installation of pen registers and trap and trace devices in the context of a foreign intelligence investigation. The fourth affords intelligence officials access to business records and other tangible items. The fifth directs the Attorney General to report to Congress on the specifics of the exercise of FISA authority. The sixth, scheduled to expire on December 30, 2012, permits the acquisition of the communications of targeted overseas individuals and entities. The seventh creates a safe harbor from civil liability for those who assist or have assisted in the collection of information relating to the activities of foreign powers and their agents.

This report is an abridged version of CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle, without the footnotes, attributions to authority, the text of ECPA or FISA, or appendices found there. The ECPA sections of the longer report are available separately as CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle, which in turn is available in abridged form, CRS Report R41734, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, by Charles Doyle. Related CRS reports include CRS Report R42725, *Reauthorization of the FISA Amendments Act*, by Edward C. Liu, and CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

## **Contents**

|   |    |
|---|----|
| Electronic Communications Privacy Act.....                    | 1  |
| Title III.....  | 1  |
| Stored Communications Act (SCA) .....                         | 4  |
| Pen Registers and Trap and Trace Devices (PR/T&T) .....       | 7  |
| Foreign Intelligence Surveillance Act.....                    | 8  |
| Foreign Intelligence Surveillance Court.....                  | 8  |
| FISA Electronic Surveillance and Physical Search Orders ..... | 9  |
| Pen Registers and Trap and Trace Devices.....                 | 11 |
| Tangible Items .....  | 11 |
| Overseas FISA Targets (Expires December 30, 2012) .....       | 12 |
| FISA Reporting Requirements.....                              | 15 |

## **Contacts**

|                                 |    |
|---------------------------------|----|
| Author Contact Information..... | 15 |
|---------------------------------|----|

This is an outline of two federal statutes: the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). Both evolved out of the shadow of the Supreme Court's Fourth Amendment jurisprudence. The courts play an essential role in both. Congress crafted both to preserve the ability of government officials to secure information critical to the nation's well-being and to ensure individual privacy. It modeled parts of FISA after features in ECPA. There are differences, however. ECPA protects individual privacy from the intrusions of other individuals. FISA has no such concern. FISA authorizes the collection of information about the activities of foreign powers and their agents, whether those activities are criminal or not. ECPA's only concern is crime.

## Electronic Communications Privacy Act

### Title III

**Prohibitions:** In Title III, ECPA begins the proposition that unless provided otherwise, it is a federal crime to engage in wiretapping or electronic eavesdropping; to possess wiretapping or electronic eavesdropping equipment; to use or disclose information obtained through illegal wiretapping or electronic eavesdropping; or to disclose information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice.

*Wiretapping:* First among these is the ban on illegal wiretapping and electronic eavesdropping that covers: (1) any person who (2) intentionally (3) intercepts, or endeavors to intercept (4) wire, oral or electronic communications (5) by using an electronic, mechanical or other device, (6) unless the conduct is specifically authorized or expressly not covered, *e.g.* (a) one of the parties to the conversation has consent to the interception, (b) the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially supervised) law enforcement or foreign intelligence gathering interception, (c) the interception occurs as part of providing or regulating communication services, (d) certain radio broadcasts, and (e) in some places, spousal wiretappers.

*Unlawful Disclosure:* Title III has three disclosure offenses. The first is a general prohibition focused on the products of an unlawful interception: (1) any person [who] (2) intentionally (3) discloses or endeavors to disclose to another person (4) the contents of any wire, oral, or electronic communication (5) having reason to know (6) that the information was obtained through the interception of a wire, oral, or electronic communication (7) in violation of 18 U.S.C. 2511(1) (8) is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper. When the illegally secured information relates to a matter of usual public concern, the First Amendment precludes a prosecution for disclosure under §2511(c). Moreover, the legislative history indicates that Congress did not intend to punish the disclosure of intercepted information that is public knowledge. Finally, the results of electronic eavesdropping authorized under Title III may be disclosed and used for law enforcement purposes and for testimonial purposes.

Title III makes it a federal crime to disclose intercepted communications under two other circumstances. It is a federal crime to disclose, with an intent to obstruct criminal justice, any information derived from lawful police wiretapping or electronic eavesdropping. A third disclosure proscription applies only to electronic communications service providers "who intentionally divulge the contents of the communication while in transmission" to anyone other

than sender and intended recipient. Violators would presumably be exposed to criminal liability under the general disclosure proscription and to civil liability.

*Unlawful Use:* The prohibition on the use of information secured from illegal wiretapping or electronic eavesdropping mirrors its disclosure counterpart: (1) any person [who] (2) intentionally (3) uses or endeavors to use to another person (4) the contents of any wire, oral, or electronic communication (5) having reason to know (6) that the information was obtained through the interception of a wire, oral, or electronic communication (7) in violation of 18 U.S.C. 2511(1), (8) is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper. The criminal and civil liability that attend unlawful use of intercepted communications in violation of paragraph 2511(1)(d) are the same as for unlawful disclosure in violation of paragraphs 2511(1)(c) or 2511(1)(e), or for unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b).

*Possession of Intercept Devices:* The proscriptions for possession and trafficking in wiretapping and eavesdropping devices are even more demanding than those that apply to the predicate offense itself. There are exemptions for service providers, government officials, and those under contract with the government, but there is no exemption for equipment designed to be used by private individuals, lawfully but surreptitiously.

**Government Access:** Title III exempts federal and state law enforcement officials from its prohibitions on the interception of wire, oral, and electronic communications under three circumstances: (1) pursuant to or in anticipation of a court order, (2) with the consent of one of the parties to the communication; and (3) with respect to the communications of an intruder within an electronic communications system. To secure a Title III interception order as part of a federal criminal investigation, a senior Justice Department official must approve the application for the court order authorizing the interception of wire or oral communications. The procedure is only available where there is probable cause to believe that the wiretap or electronic eavesdropping will produce evidence of one of a long, but not exhaustive, list of federal crimes, or of the whereabouts of a “fugitive from justice” fleeing from prosecution of one of the offenses on the predicate offense list. Any federal prosecutor may approve an application for a court order under section 2518 authorizing the interception of e-mail or other electronic communications and the authority extends to any federal felony rather than more limited list of federal felonies upon which a wiretap or bug must be predicated.

At the state level, the principal prosecuting attorney of a state or any of its political subdivisions may approve an application for an order authorizing wiretapping or electronic eavesdropping based upon probable cause to believe that it will produce evidence of a felony under the state laws covering murder, kidnaping, gambling, robbery, bribery, extortion, drug trafficking, or any other crime dangerous to life, limb or property. State applications, court orders and other procedures must at a minimum be as demanding as federal requirements.

Applications for a court order authorizing wiretapping and electronic surveillance must include the identity of the applicant and the official who authorized the application; a full and complete statement of the facts including details of the crime; a particular description of the nature, location and place where the interception is to occur; a particular description of the communications to be intercepted; the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted; a full and complete statement of the alternative investigative techniques used or an explanation of why they would be futile or dangerous; a statement of the period of time for which the interception is to be maintained and if it will not terminate upon seizure of the communications sought, a probable cause demonstration that

further similar communications are likely to occur; a full and complete history of previous interception applications or efforts involving the same parties or places; in the case of an extension, the results to date or explanation for the want of results; and any additional information the judge may require.

Before issuing an order authorizing interception, the court must find: probable cause to believe that an individual is, has, or is about to commit one or more of the predicate offenses; probable cause to believe that the particular communications concerning the crime will be seized as a result of the interception requested; that normal investigative procedures have been or are likely to be futile or too dangerous; and probable cause to believe that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

Subsections 2518(4) and (5) demand that any interception order include the identity (if known) of the persons whose conversations are to be intercepted; the nature and location of facilities and place covered by the order; a particular description of the type of communication to be intercepted and an indication of the crime to which it relates; the individual approving the application and the agency executing the order; the period of time during which the interception may be conducted and an indication of whether it may continue after the communication sought has been seized; an instruction that the order shall be executed; as soon as practicable, and so as to minimize the extent of innocent communication seized; and upon request, a direction for the cooperation of communications providers and others necessary or useful for the execution of the order.

The court orders remain in effect only as long as required but not more than 30 days. After 30 days, the court may grant 30-day extensions subject to the procedures required for issuance of the original order. During that time the court may require progress reports at such intervals as it considers appropriate. Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order. Within 90 days of the expiration of the order, those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days' advance notice to the parties.

Title III also describes conditions under which information derived from a court-ordered interception may be disclosed or otherwise used. It permits disclosure and use for official purposes by: other law enforcement officials including foreign officials; federal intelligence officers to the extent that it involves foreign intelligence information; other American or foreign government officials to the extent that it involves the threat of hostile acts by foreign powers, their agents, or international terrorists. It also allows witnesses testifying in federal or state proceedings to reveal the results of a Title III tap, provided the intercepted conversation or other communication is not privileged.

**Consequences of a Violation:** *Criminal Penalties:* Interception, use, or disclosure in violation of Title III is generally punishable by imprisonment for not more than five years and/or a fine of not more than \$250,000 for individuals and not more than \$500,000 for organizations. In addition to exemptions previously mentioned, Title III provides a defense to criminal liability based on good faith.

*Civil Liability:* Victims of a violation of Title III may be entitled to equitable relief, damages (equal to the greater of actual damages, \$100 per day of violation, or \$10,000), punitive damages, reasonable attorney's fees, and reasonable litigation costs. A majority of federal courts hold that governmental entities other than the United States may be liable for violations of §2520 and that law enforcement officers enjoy a qualified immunity from suit under §2520. The cause of action created in §2520 is subject to a good faith defense. Efforts to claim the defense by anyone other than government officials or someone working at their direction have been largely unsuccessful. Finally, the USA PATRIOT Act authorizes a cause of action against the United States for willful violations of Title III, the Foreign Intelligence Surveillance Act, or the provisions governing stored communications in 18 U.S.C. 2701-2712. Successful plaintiffs are entitled to the greater of \$10,000 or actual damages, and reasonable litigation costs.

*Administrative and Professional Disciplinary Action:* Upon a judicial or administrative finding of a Title III violation suggesting possible intentional or willful misconduct on the part of a federal officer or employee, the federal agency or department involved may institute disciplinary action. It is required to explain to its Inspector General's office if it declines to do so. Attorneys who engage in *unlawful* wiretapping or electronic eavesdropping remain subject to professional discipline in every jurisdiction. Courts and bar associations have had varied reactions to *lawful* wiretapping or electronic eavesdropping by members of the bar.

*Exclusion of Evidence:* When the Title III prohibits disclosure, the information is inadmissible as evidence before any federal, state, or local tribunal or authority. Individuals whose conversations have been intercepted or against whom the interception was directed have standing to claim the benefits of the §2515 exclusionary rule through a motion to suppress. Section 2518(10)(a) bars admission as long as the evidence is the product of (1) an unlawful interception, (2) an interception authorized by a facially insufficient court order, or (3) an interception executed in manner substantially contrary to the order authorizing the interception. Mere technical noncompliance is not enough; the defect must be of a nature that substantially undermines the regime of court-supervised interception for law enforcement purposes.

## **Stored Communications Act (SCA)**

**Prohibitions:** The SCA has two sets of proscriptions: a general prohibition and a second applicable to only certain communications providers. The general proscription makes it a federal crime to: (1) intentionally (2) either (a) access without authorization or (b) exceed an authorization to access (3) a facility through which an electronic communication service is provided (4) and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

Section 2701's prohibitions yield to several exceptions and defenses. First, the section itself declares that Subsection (a) of this section does not apply with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user; or (3) in section 2703 [requirements for government access], 2704 [backup preservation] or 2518 [court ordered wiretapping or electronic eavesdropping] of this title. Second, there are the good faith defenses provided by section 2707. Third, there is the general immunity from civil liability afforded providers under subsection 2703(e).

A second set of prohibitions appears in section 2702 and supplements those in section 2701. Section 2702 bans the disclosure of the content of electronic communications and records relating

to them by those who provide the public with electronic communication service or remote computing service. The section forbids providers to disclose the content of certain communications to anyone or to disclose related records to governmental entities. Section 2702 comes with its own set of exceptions which permit disclosure of the contents of a communication: (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517 [relating to disclosures permitted under Title III], 2511(2)(a)[relating to provider disclosures permitted under Title III for protection of provider property or incidental to service], or 2703 [relating to required provider disclosures pursuant to governmental authority] of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990; (7) to a law enforcement agency—(A) if the contents—(i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or (8) to a federal, state, or local government 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 communications relating to the emergency. The record disclosure exceptions are similar.

**Government Access:** The circumstances and procedural requirements for law enforcement access to stored wire or electronic communications and transactional records are less demanding than those under Title III. They deal with two kinds of information—often in the custody of the communications service provider rather than of any of the parties to the communication—communications records and the content of electronic or wire communications. The Stored Communications Act provides two primary avenues for law enforcement access: permissible provider disclosure (section 2702) and required provided access (section 2703). As noted earlier in the general discussion of section 2702, a public electronic communication service (ECS) provider or a public remote computing service (RCS) provider may disclose the content of a customer's communication without the consent of a communicating party to a law enforcement agency in the case of inadvertent discovery of information relating to commission of a crime, or to any government entity in an emergency situation. ECS and RCS providers may also disclose communications records to any governmental entity in an emergency situation. Federal, state, and local agencies, regardless of the nature of their missions, all qualify as governmental entities for purposes of section 2702.

Section 2702 authorizes voluntary disclosure. Section 2703 speaks to the circumstances under which ECS and RCS providers may be required to disclose communications content and related records. Section 2703 distinguishes between recent communications and those that have been in electronic storage for more than 180 days. The section insists that government entities resort to a search warrant to compel providers to supply the content of wire or electronic communications held in electronic storage for less than 180 days. It permits them to use a warrant, subpoena, or a court order authorized in subsection 2703(d) to force content disclosure with respect to communications held for more than 180 days. A subsection 2703(d) court order may be issued by a federal magistrate or by a judge qualified to issue an order under Title III. It need not be issued in the district in which the provider is located. The person whose communication is disclosed is entitled to notice, unless the court authorizes delayed notification because contemporaneous notice might have an adverse impact. Government supervisory officials may certify the need for delayed notification in the case of a subpoena.



Subsection 2703(d) authorizes issuance of an order when the governmental entity has presented specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation. Some courts have held that this “reasonable grounds” standard is a *Terry* standard, a less demanding standard than “probable cause,” and that under some circumstances this standard may be constitutionally insufficient to justify government access to provider-held e-mail. A Sixth Circuit panel has held that the Fourth Amendment precludes government access to the content of stored communications (e-mail) held by service providers in the absence of a warrant, subscriber consent, or some other indication that the subscriber has waived his or her expectation of privacy. Where the government instead secures access through a subpoena or court order as section 2703 permits, the evidence may be subject to both the Fourth Amendment exclusionary rule and the exceptions to the rule.

The SCA has two provisions which require providers to save customer communications at the government’s request. One is found in subsection 2703(f). It requires ECS and RCS providers to preserve “records and other evidence in its possession,” at the request of a governmental entity pending receipt of a warrant, court order, or subpoena. Whether providers are bound to preserve e-mails and other communications that come into their possession both before and after receipt of the request is unclear. The second preservation provision is more detailed. It permits a governmental entity to insist that providers preserve backup copies of the communications covered by a subpoena or subsection 2703(d) court order. It gives subscribers the right to challenge the relevancy of the information sought. It might also be read to require the preservation of the content of communications received by the provider both before and after receipt of the order, but the requirement that copies be made within two days of receipt of the order seems to preclude such an interpretation.

Section 2703 provides greater protection to communication content than to provider records relating to those communications. Under subsection 2703(c), a governmental entity may require a ECS or RCS provider to disclose records or information pertaining to a customer or subscriber—other than the content of a communication—under a warrant, a court order under subsection 2703(d), or with the consent of the subject of the information. An administrative, grand jury, or trial subpoena is sufficient, however, for a limited range of customer or subscriber related information. The customer or subscriber need not be notified of the record disclosure in either case. The district courts have been divided for some time over the question of what standard applies when the government seeks cell phone location information from a provider, either current or historical. The Third Circuit has held that while issuance of an order under subsection 2703(d) does not require a showing of probable cause as a general rule, the circumstances of a given case may require it.

In *United States v. Jones*, five members of the Supreme Court seemed to suggest that a driver has a reasonable expectation that authorities must comply with the demands of the Fourth Amendment before acquiring access to information that discloses the travel patterns of his car over an extended period of time. There, the Court unanimously agreed that the agents’ attachment of a tracking device to Jones’ car and long-term capture of the resulting information constituted a Fourth Amendment search. For four Justices, placement of the device constituted a physical intrusion upon a constitutionally protected area. For four others, long-term tracking constituted a breach of Jones’ reasonable expectation of privacy. For the ninth Justice, the activity constituted a Fourth Amendment search under either rationale. It remains to be seen whether the Supreme Court’s decision in *Jones* will contribute to resolution of the issue.

**Consequences:** Breaches of the unauthorized access prohibitions of section 2701 expose offenders to possible criminal, civil, and administrative sanctions. Violations committed for malicious, mercenary, tortious, or criminal purposes are punishable by imprisonment for not more than five years (not more than 10 years for a subsequent conviction) and/or a fine of not more than \$250,000 (not more than \$500,000 for organizations); lesser transgressions, by imprisonment for not more than one year (not more than five years for a subsequent conviction) and/or a fine of not more than \$100,000. Victims of a violation of subsection 2701(a) have a cause of action for equitable relief, reasonable attorneys' fees and costs, and damages equal to the amount of any offender profits added to the total of the victim's losses (but not less than \$1,000 in any event).

Violations by the United States may give rise to a cause of action and may result in disciplinary action against offending officials or employees under the same provisions that apply to U.S. violations of Title III. Unlike violations of Title III, however, there is no statutory prohibition on disclosure or use of the information through a violation of section 2701; nor is there a statutory rule for the exclusion of evidence as a consequence of a violation. Yet, violations of SCA, which also constitute violations of the Fourth Amendment, will trigger both the Fourth Amendment exclusionary rule and the exceptions to that rule.

No criminal penalties attend a violation of voluntary provider disclosure prohibitions of section 2702. Yet, ECS and RCS providers—unable to claim the benefit of one of the section's exceptions, of the good faith defense under subsection 2707(e), or of the immunity available under subsection 2703(e)—may be liable for civil damages, costs, and attorneys' fees under section 2707 for any violation of section 2702.

## **Pen Registers and Trap and Trace Devices (PR/T&T)**

**Prohibitions:** A trap and trace device identifies the source of incoming calls, and a pen register indicates the numbers called from a particular instrument. Since they did not allow the user to overhear the "contents" of the phone conversation or to otherwise capture the content of a communication, they were not considered interceptions within the reach of Title III prior to the enactment of ECPA. Although Congress elected to expand the definition of interception, it chose to regulate these devices beyond the boundaries of Title III for most purposes. Nevertheless, the Title III wiretap provisions apply when, due to the nature of advances in telecommunications technology, pen registers and trap and trace devices are able to capture wire communication "content."

Subsection 3121(a) outlaws installation or use of a pen register or trap and trace device, except under one of seven circumstances: (1) pursuant to a court order issued under sections 3121-3127; (2) pursuant to a Foreign Intelligence Surveillance Act (FISA) court order; (3) with the consent of the user; (4) when incidental to service; (5) when necessary to protect users from abuse of service; (6) when necessary to protect providers from abuse of service; or (7) in an emergency situation.

**Government Access:** Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information that it will provide is relevant to a pending criminal investigation. The order may be issued by a judge of "competent jurisdiction" over the offense under investigation, including a federal magistrate judge. Senior Justice Department or state prosecutors may approve the installation and use of a pen register or trap and trace device prior to the issuance of court authorization in emergency cases that involve either an organized crime conspiracy, an immediate danger of death or serious injury, a threat to national security, or a

serious attack on a “protected computer.” Emergency use must end within 48 hours, or sooner if an application for court approval is denied. Federal authorities have applied for court orders, under the Stored Communications Act (18 U.S.C. 2701-2712) and the trap and trace authority of 18 U.S.C. 3121-3127, seeking to direct communications providers to supply them with the information necessary to track cell phone users in conjunction with an ongoing criminal investigation. Thus far, their efforts have met with mixed success.

**Consequences:** The use or installation of pen registers or trap and trace devices by anyone other than the telephone company, service provider, or those acting under judicial authority is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than \$100,000 (\$200,000 for an organization). Subsection 3124(e) creates a good faith defense for reliance upon a court order under subsection 3123(b), an emergency request under subsection 3125(a), “a legislative authorization, or a statutory authorization.” There is no accompanying exclusionary rule, and consequently a violation of section 3121 will not serve as a basis to suppress any resulting evidence.

Moreover, unlike violations of Title III, there is no requirement that the target of an order be notified upon the expiration of the order; nor is there a separate federal private cause of action for victims of a pen register or trap and trace device violation. One court, in order to avoid First Amendment concerns, has held that the statute precludes imposing permanent gag orders upon providers. Nevertheless permitting providers to disclose the existence of an order to a target does not require them to do so. Some of the states have established a separate criminal offense for unlawful use of a pen register or trap and trace device, yet most of these seem to follow the federal lead and have not established a separate private cause of action for unlawful installation or use of the devices.

## **Foreign Intelligence Surveillance Act**

The Foreign Intelligence Surveillance Act (FISA) authorizes special court orders for several purposes: electronic surveillance, physical searches, installation and use of pen registers and trap and trace devices, and orders to disclose tangible items. It once authorized surveillance orders which targeted the communications of persons overseas. Its replacement provisions for the review of orders directed at persons abroad expire on December 30, 2012. FISA insists that Congress be informed as to the extent that its authority has been used and establishes a safe harbor for those who help carry out its orders.

## **Foreign Intelligence Surveillance Court**

The Foreign Intelligence Surveillance Court (the FISA court) is a creature of FISA. The FISA court consists of eleven federal district court judges from throughout the country, designated by the Chief Justice of the United States. The individual members of the court receive and act upon FISA order applications. Federal magistrate judges, designated by the Chief Justice, may also perform those functions with respect to pen register/trap and trace orders. Members of the FISA court, sitting in panels, pass upon challenges associated with the execution of tangible item and overseas targeting orders. These panels also rule upon requests to modify or set aside gag orders issued in connection with the execution of tangible item orders. The government may appeal the denial of a FISA application to a Foreign Intelligence Surveillance Court of Review made up of three federal judges designated by the Chief Justice.

## **FISA Electronic Surveillance and Physical Search Orders**

**Government Access:** The FISA electronic surveillance and physical search components use generally parallel procedures. Both draw from their law enforcement counterparts, but with important differences. A FISA electronic surveillance or physical search application must include (1) the identity of the individual submitting the application; (2) the identity or a description of the person whose communications are to be intercepted; (3) an indication of (a) why the person is believed to be a foreign power or the agent of a foreign power, and (b) why foreign powers or their agents are believed to use the targeted facilities or places; (4) a summary of the minimization procedures to be followed; (5) a description of the communications to be intercepted and the information sought; (6) certification by a senior national security or senior defense official designed by the President that (a) the information sought is foreign intelligence information, (b) a significant purpose of interception is to secure foreign intelligence information, (c) the information cannot reasonably be obtained using alternative means; (7) a summary statement of the means of accomplishing the interception (including whether a physical entry will be required); (8) a history of past interception applications involving the same persons, places, or facilities; and (9) the period of time during which the interception is to occur, whether it will terminate immediately upon obtaining the information sought, and if not, the reasons why interception thereafter is likely to be productively intercepted.

The judges issue orders approving electronic surveillance or physical searches upon a finding that the application requirements have been met and that there is probable cause to believe that the target is a foreign power or the agent of a foreign power and that the targeted places or facilities are used by foreign powers or their agents.

Orders approving electronic surveillance must (1) specify: (a) the identity or a description of the person whose communications are to be intercepted, (b) the nature and location of the targeted facilities or places, if known, (c) type of communications or activities targeted and the kind of information sought, (d) the means by which interception is to be accomplished and whether physical entry is authorized, (e) the tenure of the authorization, and (f) whether more than one device are to be used and if so their respective ranges and associated minimization procedures; (2) require: (a) that minimization procedures be adhered to, (b) upon request, that carriers and others provide assistance, and (c) that those providing assistance observe certain security precautions, and be compensated; (3) direct the applicant to advise the court of the particulars relating to surveillance directed at additional facilities and places when the order permits surveillance although the nature and location of targeted facilities and places were unknown at the time of issuance; and (4) expire when its purpose is accomplished but not later than after 90 days generally (after 120 days in the case of certain foreign agents and after a year in the case of foreign governments or their entities or factions of foreign nations) unless extended (extensions may not exceed one year).

As in the case of law enforcement wiretapping and electronic eavesdropping, there is authority for interception and physical searches prior to approval in emergency situations. However, there is also statutory authority for foreign intelligence surveillance interceptions and physical searches without the requirement of a court order when the targets are limited to communications among or between foreign powers or involve nonverbal communications from places under the open and exclusive control of a foreign power. The second of these is replete with reporting requirements to Congress and the FISA court. These and the twin war time exceptions may be subject to constitutional limitations, particularly when Americans are the surveillance targets.

FISA has detailed provisions governing the use of the information acquired through the use of its surveillance or physical search authority that include confidentiality requirements; notice of required Attorney General approval for disclosure; notice to the “aggrieved” of the government’s intention to use the results as evidence; suppression procedures; inadvertently captured information; notification of emergency surveillance or search for which no FISA order was subsequently secured; and clarification that those who execute FISA surveillance or physical search orders may consult with federal and state law enforcement officers.

*Exclusivity:* Title III has long declared that it should not be construed to confine governmental activities authorized under FISA, but that the two—Title III and FISA—are the exclusive authority under which governmental electronic surveillance may be conducted in this country. The Justice Department suggested, however, that in addition to the President’s constitutional authority the Authorization for the Use of Military Force Resolution, enacted in response to the events of September 11, 2001, established an implicit exception to the exclusivity requirement. Section 102 of 2008 FISA Amendments Act seeks to overcome the suggestion by establishing a second exclusivity section which declares that exceptions may only be created by explicit statutory language.

**Prohibitions and Consequences:** *Criminal:* It is a federal crime for federal officials to abuse their authority under either the FISA electronic surveillance or physical search provisions. The prohibitions cover illicit surveillance and searches as well as the use or disclosure of such unlawful activities. Violations are punishable by a fine and/or imprisonment for not more than five years. Federal law enforcement and investigative officers enjoy the benefit of a defense, if they are acting under the authority of warrant or court order.

*Civil:* Violations may also expose the offender to civil liability. Those directed to assist authorities in execution of an electronic surveillance or physical search order are immune from civil suit. Moreover, even in the absence of a court order, the 2008 FISA Amendments Act bars the initiation or continuation of civil suits in either state or federal court based on charges that the defendant assisted any of the U.S. intelligence agencies. Dismissal is required upon the certification of the Attorney General that the person either: (1) did not provide the assistance charged; (2) provided the assistance under order of the FISA court; (3) provided the assistance pursuant to a national security letter issued under 18 U.S.C. 2709; (4) provided the assistance pursuant to 18 U.S.C. 2511(2)(a)(ii)(B) and 2518(7) under assurances from the Attorney General or a senior Justice Department official, empowered to approve emergency law enforcement wiretaps, that no court approval was required; (5) provided the assistance in response to a directive from the President through the Attorney General relating to communications between or among foreign powers pursuant to 50 U.S.C. 1802(a)(4); (6) provided the assistance in response to a directive from the Attorney General and the Director of National Intelligence relating to the acquisition of foreign intelligence information targeting non-U.S. persons thought to be overseas pursuant to 50 U.S.C. 1881a(h); or (7) provided the assistance in connection with intelligence activities authorized by the President between September 11, 2001, and January 17, 2007, relating to terrorist attacks against the United States.

Only telecommunications carriers, electronic service providers, and other communication service providers may claim the protection afforded those who assisted activities authorized between 9/11 and January 17, 2007. The group which may claim protection for assistance supplied under other grounds is larger. It includes not only communication service providers but also any “landlord, custodian or other person” ordered or directed to provide assistance. The Attorney General’s certification is binding if supported by substantial evidence, and the court is to consider

challenges and supporting evidence *ex parte* and *in camera* where the Attorney General asserts that disclosure would harm national security. Cases filed in state court may be removed to federal court. The courts have rejected arguments that immunity procedure violates the Due Process Clause, the First Amendment, separation of powers, and the Administrative Procedure Act in multi-district civil litigation arising out of the National Security Agency program.

With the reduced availability of individual defendants, the USA PATRIOT Act amendments afford victims of any improper use of information secured under a FISA surveillance, physical search, or pen register order a cause of action against the United States for actual or statutory damages. No comparable cause of action against the United States exists for other FISA violations.

*Evidentiary:* FISA also has its own exclusionary rules for evidence derived from unlawful FISA electronic surveillance or physical searches. Nevertheless, Congress anticipated, and the courts have acknowledged, that lawful surveillance and searches conducted under FISA for foreign intelligence purposes may result in admissible evidence of a crime.

## **Pen Registers and Trap and Trace Devices**

**Government Access:** FISA pen register and trap and trace procedures are similar to those of their law enforcement counterparts, but with many of the attributes of other FISA provisions. The orders may be issued either by a member of the FISA court or by a FISA magistrate upon the certification of a federal officer that the information sought is likely to be relevant to an investigation of international terrorism or clandestine intelligence activities. The order may direct service providers to supply customer information related to the order. The statute allows the Attorney General to authorize emergency installation and use as long as an application is filed within 48 hours, and restricts the use of any resulting evidence if an order is not subsequently granted. The provisions for use of the information acquired run parallel to those that apply to FISA surveillance and physical search orders.

**Prohibition and Consequences:** The pen register/trap and trace portion of FISA declares that information acquired by virtue of a FISA pen register or trap and trace order may only be used and disclosed for lawful purposes and only consistent with FISA's use restrictions. It is a federal crime to install or use a pen register or trap and trace device unless authorized to do so under either ECPA or FISA. Offenders face the prospect of imprisonment for not more than one year and/or a fine of not more than \$100,000. Good faith reliance on a statutory authorization, such as the authority FISA provides, constitutes a defense. Those who assist are immune from civil liability, but victims of the unlawful use of information derived from a FISA pen register or trap and trace device order have a cause of action against the United States. The exclusionary rule for a FISA pen register or trap and trace order is comparable to that which applies in the case of evidence derived from FISA electronic surveillance or a FISA physical search.

## **Tangible Items**

FISA's tangible item orders are perhaps its most interesting feature. Prior to the USA PATRIOT Act, senior FBI officials could approve an application to the FISA court for an order authorizing common carriers, or public accommodation, storage facility, or vehicle rental establishments to release their business records based upon certification of a reason to believe that the records pertained to a foreign power or the agent of a foreign power. The USA PATRIOT Act and later the

USA PATRIOT Improvement and Reauthorization Act temporarily rewrote the procedure. In its temporary form, it requires rather than authorizes access; it is predicated upon relevancy rather than probable cause; it applies to all tangible property (not merely business records); and it applies to the tangible property of both individuals or organizations, commercial and otherwise. It is limited, however, to investigations conducted to secure foreign intelligence information or to protect against international terrorism or clandestine intelligence activities. Recipients are prohibited from disclosing the existence of the order, but are expressly authorized to consult an attorney with respect to their rights and obligations under the order. They enjoy immunity from civil liability for good faith compliance. They may challenge the legality of the order and/or ask that its disclosure restrictions be lifted or modified. The grounds for lifting the secrecy requirements are closely defined, but petitions for reconsideration may be filed annually. The decision to set aside, modify, or let stand either the disclosure restrictions of an order or the underlying order itself are subject to appellate review.

### **Overseas FISA Targets (Expires December 30, 2012)**

The 2008 FISA Amendments Act established a temporary set of three procedures which authorize the acquisition of foreign intelligence information by targeting an individual or entity thought to be overseas. One, 50 U.S.C. 1881a, applies to the targeting of an overseas person or entity that is not a U.S. person. Another, 50 U.S.C. 1881b, covers situations when the American target is overseas but the gathering involves electronic communications or stored electronic communications or data acquired in this country. The third, 50 U.S.C. 1881c, applies to situations when the American target is overseas, but section 1881b is not available, either because acquisition occurs outside of the United States or because it involves something other than electronic surveillance or the acquisition of stored communications or data, e.g., a physical search.

In the case of targets who are not U.S. persons, section 1881a(a) declares “upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” It makes no mention of authorizing acquisition. It merely speaks of targeting with an eye to acquisition. Moreover, it gives no indication of whether the anticipated methods of acquisition include the capture of a target’s communications, of communications relating to a target, of communications of a person or entity related to the target, or information concerning one of the three. The remainder of the section, however, seems to dispel some of the questions. Section 1881a is intended to empower the Attorney General and the Director of National Intelligence to authorize the acquisition of foreign intelligence information and the methods that may be used to the capture of communications and related information.

The procedure begins either with a certification presented to the FISA court for approval or with a determination by the two officials that exigent circumstances warrant timely authorization prior to court approval. In the certification process, they must assert in writing and under oath that (1) a significant purpose of the effort is the acquisition of foreign intelligence information; (2) the effort will involve the assistance of an electronic communication service provider; (3) the court has approved, or is being asked to approve, procedures designed to ensure that acquisition is limited to targeted persons found outside the United States and to prevent the capture of communications in which all the parties are within the United States; (4) minimization

procedures, which the court has approved or is being asked to approve and which satisfy the requirements for such procedures in the case of FISA electronic surveillance and physical searches, will be honored; (5) guidelines to ensure compliance with limitations imposed in the section have been adopted and the limitations will be observed; and (6) these procedures and guidelines are consistent with Fourth Amendment standards. The certification is to be accompanied by a copy of the targeting and minimization procedures, any supporting affidavits from senior national security officials, an indication of the effective date of the authorization, and a notification of whether pre-approval emergency authorization has been given. The certification, however, need not describe the facilities or places at which acquisition efforts will be directed.

The limitations preclude intentionally targeting a person in the United States, “reverse targeting” (intentionally targeting a person overseas purpose of targeting a person within the United States), intentionally targeting a U.S. person outside the United States, intentionally acquiring a communication in which all of the parties are in the United States, or conducting the acquisition in a manner contrary to the demands of the Fourth Amendment. The Attorney General, in consultation with the Director of National Intelligence, is obligated to promulgate targeting and minimization procedures and guidelines to ensure that the section’s limitations are observed. The minimization procedures must satisfy the standards required for similar procedures required for FISA electronic surveillance and physical searches. The targeting procedures must be calculated to avoid acquiring communications in which all of the parties are in the United States and to confine targeting to persons located outside the United States. Both are subject to review by the FISA court for sufficiency when it receives the request to approve the certification. Copies of the guidelines, which also provide directions concerning the application for FISA court approval under the section, must be supplied to court and to the congressional intelligence and judiciary committees.

The Attorney General and Director of National Intelligence may instruct an electronic communications service provider to assist in the acquisition. Cooperative providers are entitled to compensation and are immune from suit for their assistance. They may also petition the FISA court to set aside or modify the direction for assistance, if it is unlawful. The Attorney General may petition the court to enforce a directive against an uncooperative provider. The court’s decisions concerning certification approval, modification of directions for assistance, and enforcement of the directives are each appealable to the Foreign Intelligence Court of Review and on certiorari to the Supreme Court. Except with respect to disclosure following a failure to secure court approval of an emergency authorization, section 1806, discussed earlier, governs the use of information obtained under the authority of section 1881a.

When the overseas target is an American individual or entity and acquisition is to occur in this country, the court may authorize acquisition by electronic surveillance or by capturing stored electronic communications or data under section 1881b. The Attorney General must approve the application which must be made under oath and indicate: (1) the identity of the applicant; (2) the identity, if known, or description of the American target; (3) the facts establishing that reason to believe that the person is overseas and a foreign power or its agent, officer, or employee; (4) the applicable minimization procedures; (5) a description of the information sought and the type of communications or activities targeted; (6) certification by the Attorney General or a senior national security or defense official that (a) foreign intelligence information is to be sought, (b) a significant purpose of the effort is to obtain such information, (c) the information cannot otherwise reasonably be obtained (and the facts upon which this conclusion is based), and (d) the nature of the information (e.g., relating to terrorism, sabotage, the conduct of U.S. foreign affairs, etc.)(and the facts upon which this conclusion is based); (7) the means of acquisition and whether



physical entry will be necessary; (8) the identity of the service providing assisting (targeted facilities and premises need not be identified); (9) a statement of previous applications relating to the same American and actions taken; (10) the proposed tenure of the order (not to exceed 90 days), and (11) any additional information the FISA court may require.

The court must issue an acquisition order upon a finding that the application satisfies statutory requirements, the minimization procedures are adequate, and there is probable cause to believe that the American target is located overseas and is a foreign power or its agent, officer, or employee. The court must explain in writing any finding that the application's assertion of probable cause, minimization procedures, or certified facts is insufficient. Such findings are appealable to the Foreign Intelligence Surveillance Court of Review and under certiorari to the Supreme Court. The court's order approving acquisition is to include the identity or description of the American target, the type of activities targeted, the nature of the information sought, the means of acquisition, and duration of the order. The order will also call for compliance with the minimization procedures, and when appropriate, for confidential, minimally disruptive provider assistance, compensated at a prevailing rate. Providers are immune from civil liability for any assistance they are directed to provide.

As in other instances, in emergency cases the Attorney General may authorize acquisition pending approval of the court. The court must be notified of the Attorney General's decision and the related application must be filed within seven days. If emergency acquisition is not judicially approved subsequently, no resulting evidence may be introduced in any judicial, legislative, or regulatory proceedings unless the target is determined not to be an American, nor may resulting information be shared with other federal officials without the consent of the target, unless the Attorney General determines that the information concerns a threat of serious bodily injury. Except with respect to disclosure following a failure to court approval of an emergency authorization, section 1806, discussed earlier, governs the use of information obtained under the authority of section 1881a.

The second provision for targeting an American overseas in order to acquire foreign intelligence information, section 1881c, is somewhat unique. Both FISA electronic surveillance and Title III have been understood to apply only to interceptions within the United States. Neither has been thought to apply overseas. Section 1881c, however, may be used for acquisitions outside the United States. Moreover, it may be used for acquisitions inside the United States as long as the requirements that would ordinarily attend such acquisition are honored.

Otherwise, section 1881c features many of the same application, approval, and appeal provisions as section 1881b. Authorization is available under a court order or in emergency circumstances under the order of the Attorney General. Acquisition activities must be discontinued during any period when the target is thought to be in the United States. Unlike 1881b, however, it is not limited to electronic surveillance or the acquisition of stored electronic information. Moreover, it declares that in the case of acquisition abroad recourse to a court order need only be had when the target American, found overseas, has a reasonable expectation of privacy and a warrant would be required if the acquisition efforts had taken place in the United States and for law enforcement purposes.

A challenge to the constitutionality of section 1881a was initially dismissed because the district court did not believe the plaintiffs had shown that they had standing (i.e., a sufficient individual injury attributable to execution of the statute's authority). The Second Circuit disagreed. The Supreme Court has agreed to consider the case.

## **FISA Reporting Requirements**

Every six months, the Attorney General must report on the use of FISA authority. Recipients are the House and Senate Judiciary Committees and the House and Senate Intelligence committees. In a manner consistent with the protection of national security, the transmission must provide: (1) the number of persons targeted under: (a) FISA electronic surveillance orders, (b) FISA physical search orders, (c) FISA pen register/trap and trace orders, (d) FISA tangible item orders, and (e) FISA acquisitions relating to U.S. persons overseas; (2) the number of persons covered as lone wolf terrorists; (3) the number of times the Attorney General has authorized the use of FISA material in a criminal proceeding; (4) a summary of the significant legal interpretations of the FISA court or the FISA Court of Review; and (5) copies of the decisions, orders, and opinions of those courts.

## **Author Contact Information**

Gina Stevens  
Legislative Attorney  
gstevens@crs.loc.gov, 7-2581

Charles Doyle  
Senior Specialist in American Public Law  
cdoyle@crs.loc.gov, 7-6968