
# Privacy: An Abridged Overview of the Electronic Communications Privacy Act

**Charles Doyle**
Senior Specialist in American Public Law

October 9, 2012

**Congressional Research Service**
7-5700
www.crs.gov
R41734

**CRS Report for Congress**
*Prepared for Members and Committees of Congress*

# Summary

This report provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA).

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); civil liability for damages, attorneys' fees and possibly punitive damages; disciplinary action against any attorneys involved; and suppression of any derivative evidence. Congress has created separate, but comparable, protective schemes for electronic communications (e.g., email) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, and install and use pen registers and trap and trace devices for law enforcement purposes under ECPA and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act.

This report is an abridged version of CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle, without the footnotes, quotations, attributions of authority, or appendixes found there. The longer report also serves as the first section of CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle, which examines both ECPA and the Foreign Intelligence Surveillance Act (FISA). It too is available in abridged form as CRS Report 98-327, *Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

# Contents



## Contacts

# Introduction

This is an outline of the Electronic Communications Privacy Act (ECPA). ECPA consists of three parts. The first, sometimes referred to as Title III, outlaws the unauthorized interception of wire, oral, or electronic communications. It also establishes a judicial supervised procedure to permit such interceptions for law enforcement purposes. The second, the Stored Communications Act, focuses on the privacy of, and government access to, stored electronic communications. The third creates a procedure for governmental installation and use of pen registers as well as trap and trace devices. It also outlaws such installation or use except for law enforcement and foreign intelligence investigations.

# 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 email 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 email. A Sixth Circuit panel has held that the Fourth Amendment precludes government access to the content of stored communications (email) 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 emails 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 allowed 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.

## Author Contact Information

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