Privacy: An Abridged Overview of the Electronic Communications Privacy Act

Charles Doyle
Senior Specialist in American Public Law

March 30, 2011

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

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

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); in civil liability for damages, attorneys' fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in 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 form of CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle, without footnotes, quotations, attributions, or appendixes found in the longer version.

Contents

Contacts

Introduction

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA). ECPA consists of three parts: a revised Title III; the Stored Communications Act (SCA); and provisions governing the installation and use of trap and trace devices and pen registers.

Illegal Wiretapping and Electronic Eavesdropping

Unless otherwise provided, Title III outlaws wiretapping and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice. At the heart of Title III lies the prohibition against illegal wiretapping and electronic eavesdropping, 18 U.S.C. 2511(1), that bans: any person from intentionally intercepting, or endeavoring to intercept, wire, oral or electronic communications by using an electronic, mechanical or other device unless the conduct is specifically authorized or expressly not covered, for example, one of the parties to the conversation has consent to the interception, the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially supervised) law enforcement or foreign intelligence gathering interception, the interception occurs as part of providing or regulating communication services, certain radio broadcasts, and in some places, spousal wiretappers.

Intentionally: The prohibition applies to "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Conduct can only violate Title III if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed. He need not be shown to have known, however, that his conduct was unlawful. Interception "means the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other devices." Yet, it does not include instances where an individual simply reads or listens to a previously intercepted communication, regardless of whether additional conduct may implicate the prohibitions on use or disclosure.

Intercepts: Once limited to aural acquisitions, ECPA enlarged the definition so that it is no longer limited to interceptions of communications that can be heard. The change complicates the question of whether the wiretap, stored communications, or trap and trace portions of the ECPA govern the legality of various means of capturing information relating to a communication. The analysis might seem to favor wiretap coverage when it begins with an examination of whether an "interception" has occurred. Yet, there is little consensus over when an interception occurs; that is, whether "interception" as used in section 2511 contemplates surreptitious acquisition, either contemporaneous with transmission, or whether such acquisition may occur anytime before the initial cognitive receipt of the contents by the intended recipient, or under some other conditions.

Content: The interceptions proscribed in Title III are confined to those that capture a communication's "content," that is, "information concerning [its] substance, purport, or meaning." Trap and trace devices and pen registers once captured only information relating to the source and addressee of a communication, not its content. That is no longer the case. The "post-cut-through dialed digit features" of contemporary telephone communications now transmit communications in such a manner that the use of ordinary pen register or trap and trace devices

will capture both non-content and content. As a consequence, a few courts have held, either as a matter of statutory construction or constitutional necessity, that the authorities must rely on a Title III wiretap order rather than a pen register/trap and trace order if such information will be captured.

By device: The statute does not cover common law "eavesdropping," but only interceptions "by electronic, mechanical or other device." The term includes computers, but it is defined so as not to include hearing aids or extension telephones in normal use (use in the "ordinary course of business"). Whether an extension phone has been installed and is being used in the ordinary course of business or in the ordinary course of law enforcement duties, so that it no longer constitutes an interception device for purposes of Title III and comparable state laws, has proven a somewhat vexing question.

Communications: An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms—telephone (wire), face to face (oral), and computer (electronic). Thus, silent video surveillance is ordinarily considered beyond ECPA's reach.

Exemptions: Consent interceptions are common, controversial and have a history all their own. The early bans on divulging telegraph or telephone messages had a consent exception. The Supreme Court upheld consent interceptions against Fourth Amendment challenge both before and after the enactment of Title III. The argument in favor of consent interceptions has always been essentially that a speaker risks the indiscretion of his listeners and holds no superior legal position simply because a listener elects to record or transmit his statements rather than subsequently memorializing or repeating them. Wiretapping or electronic eavesdropping by either the police or anyone else with the consent of at least one party to the conversation is not unlawful under the federal statute. These provisions do no more than shield consent interceptions from the sanctions of federal law; they afford no protection from the sanctions of state law. Many of the states recognize comparable exceptions, but some only permit interception with the consent of *all* parties to a communication.

Under federal law, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument. This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to be protected. Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.

Private consent interceptions may not be conducted for a criminal or tortious purpose. Some state wiretap laws do not recognize a one party consent exception. There, interception with the consent of but one party to the conversation is a violation of state law. But the federal exception is available as long as the *purpose* of the interception was neither criminal nor tortious—though the *means* may have been. At one time, the limitation encompassed interceptions for criminal, tortious, *or* otherwise injurious purposes, but ECPA dropped the reference to injurious purposes for fear that First Amendment values might be threatened should the clause be read to outlaw consent interceptions conducted to embarrass.

Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress

signals, tone-only pagers, marine radio and citizen band radio transmissions, and interceptions necessary to identify the source of any transmission, radio or otherwise, disrupting communications satellite broadcasts.

Government officials enjoy an exemption when acting under judicial authority, whether that authority is provided for in Title III for federal and state law enforcement officers acting under a court order; acting in an emergency situation pending issuance of a court order; acting under the authority of Title III in the case of communications of an intruder in a communications system acting with the approval of the system provider; acting under the authority of the Foreign Intelligence Surveillance Act, or acting under the separate provisions according them the use of pen registers and trap and trace devices.

There is a general exemption for those associated with supplying communications services, the telephone company, switchboard operators, and the like. The exemption not only permits improved service and lets the telephone company protect itself against fraud, but it allows for assistance to federal and state officials operating under a judicially supervised interception order, and for the regulatory activities of the Federal Communications Commission.

A few courts recognize a "vicarious consent" exception under which a custodial parent may secretly record the conversations of his or her minor child in the interest of protecting the child. Although rejected by most, a handful of federal courts have held that Title III does not preclude one spouse from wiretapping or electronically eavesdropping upon the other, a result other courts have sometimes reached through the telephone extension exception discussed above.

Disclosures: Although often overlooked, it is also a federal crime to disclose information obtained from illicit wiretapping or electronic eavesdropping: "any person [who] intentionally discloses or endeavors to disclose to another person the contents of any wire, oral, or electronic communication having reason to know that the information was obtained through the [unlawful] interception of a wire, oral, or electronic communication" is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper, 18 U.S.C. 2511(1)(c). The results of electronic eavesdropping authorized under Title III may be disclosed and used for law enforcement purposes and for testimonial purposes. It is also 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, 18 U.S.C. 2511(3), applies only to electronic communications service providers to the public "who intentionally divulge the contents of the communication while in transmission" to anyone other than sender and intended recipient. Although subsection 2511(3) provides no specific sanctions, violators would presumably be exposed to criminal liability under the general disclosure proscription, 18 U.S.C. 2511(1)(c), and to civil liability under 18 U.S.C. 2520.

The prohibition on the use of information secured from illegal wiretapping or electronic eavesdropping mirrors the disclosure provision. the available case law under the use prohibition of paragraph 2511(1)(d) is scant, and the section has rarely been invoked except in conjunction with the disclosure prohibition of paragraph 2511(1)(c).

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.

Title III—Government Access

Each of the prohibitions mentioned above recognizes a procedure for government use notwithstanding the general ban, usually under judicial supervision. Although the influence of the Fourth Amendment is reflected in each of three chapters—chapter 119 (Title III), chapter 121 (Stored Communications Act), and chapter 206 (pen registers and trap & trace devices)—the procedures of the three are distinctive.

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, 18 U.S.C. 2516(1)(*l*). 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.

Compliance with these procedures may be postponed briefly until after the interception effort has begun, upon the approval of senior Justice Department officials in emergency cases involving organized crime or national security threatening conspiracies or involving the risk of death or serious injury.

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.

Without a Title III order and without offending Title III, authorities may intercept the wire, oral, or electronic communications, it they have the consent of one of the parties to the communication. As noted earlier, consent may be either explicitly or implicitly given.

Little judicial or academic commentary accompanies the narrow "computer trespasser" justification for governmental interception of electronic communications in paragraph 2511(2)(i). The paragraph originated as a temporary provision in the USA PATRIOT Act, and seems designed to enable authorities to track intruders who would surreptitiously use the computer systems of others to cover their trail.

Title III –Consequences of a Violation

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. The same penalties apply to the unlawful capture of cell phone and cordless phone conversations, since the Homeland Security Act repealed the reduced penalty provisions that at one time applied to the unlawful interceptions using radio scanners and the like. There is a reduced penalty, however, for filching satellite communications as long as the interception is not conducted for criminal, tortious, nor mercenary purposes: unauthorized interceptions are broadly proscribed subject to an exception for unscrambled transmissions and are subject to the general five-year penalty, but interceptions for neither criminal, tortious, nor mercenary purposes subject offenders to only civil punishment. Equipment used to wiretap or eavesdrop in violation of Title III is subject to confiscation by the United States, either in a separate civil proceeding or as part of the prosecution of the offender. In addition to exemptions previously mentioned, Title III provides a defense to criminal liability based on good faith.

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 a court may decline to award damages, attorneys' fees and costs, but a few still consider such awards mandatory. In addition, a majority hold that governmental entities other than the United States may be liable for violations of section 2520 and that law enforcement officers enjoy a qualified immunity from suit under section 2520.

The cause of action created in section 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.

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.

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.

When the federal wiretap statute prohibits disclosure, the information is inadmissible as evidence before any federal, state, or local tribunal or authority, 18 U.S.C. 2515. Individuals whose conversations have been intercepted or against whom the interception was directed have standing to claim the benefits of the section 2515 exclusionary rule through a motion to suppress under 18 U.S.C. 2518(10)(a). Paragraph 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.

Although the Supreme Court has held that section 2515 may require suppression in instances where the Fourth Amendment exclusionary rule would not, some of the lower courts have recognized the applicability of the good faith exception to the Fourth Amendment exclusionary rule in section 2515 cases. Other courts have held, moreover, that the fruits of an unlawful wiretapping or electronic eavesdropping may be used for impeachment purposes.

The admissibility of tapes or transcripts of tapes of intercepted conversations raise a number of questions quite apart from the legality of the interception. As a consequence of the prerequisites required for admission, privately recorded conversations are more likely to be found inadmissible than those recorded by government officials. Admissibility will require the party moving for admission to show that the tapes or transcripts are accurate, authentic and trustworthy. For some courts this demands a showing that, "(1) the recording device was capable of recording the events offered in evidence; (2) the operator was competent to operate the device; (3) the recording is authentic and correct; (4) changes, additions, or deletions have not been made in the recording; (5) the recording has been preserved in a manner that is shown to the court; (6) the speakers on the tape are identified; and (7) the conversation elicited was made voluntarily and in good faith, without any kind of inducement."

Stored Electronic Communications (SCA)

In its original form Title III was ill-suited to ensure the privacy of those varieties of modern communications which are equally vulnerable to intrusion when they are at rest as when they are in transmission. Surreptitious "access" is as least as great a threat as surreptitious "interception" to the patrons of electronic mail (email), electronic bulletin boards, voice mail, pagers, and remote computer storage.

Accordingly, ECPA, in the Stored Communications Act (SCA), bans surreptitious access to communications at rest, although it does so beyond the confines that apply to interception. These separate provisions afford protection for email, voice mail, and other electronic communications only somewhat akin to that available for telephone and face to face conversations under Title III. 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: intentionally either access without authorization or exceed an authorization to access a facility through which an electronic communication service is provided and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system. The prohibition extends only to "intentional" violations, that is, violations where the defendant had as a conscious objective the forbidden conduct and proscribed result. The offense has three essential components: (1) access to, (2) a facility through which service is supplied, and (3) consequences (obtain, alter, prevent access to a wire or electronic communication). The first requires either unauthorized access or access in excess of authorization. The third requires either acquisition or alteration of an electronic communication or denial of access to it. The courts have encountered little difficulty in determining whether a defendant's conduct constitutes obtaining, altering, or preventing access to a communication. They have divided, however, over cases in which the defendant was granted access to a

communication but used access for the purposes other than that for which it was authorized. The question is less divisive when the grant of access is expressly limited or when an individual with authorized access provides an outsider with his user name and password.

The "facility through which an electronic communication service is provided" need not be one made available to the public; but includes as well facilities through which a private employer provides electronic communication services to his employees. The section only protects communications while "in electronic storage" in a facility through which electronic communications service is provided. "Electronic storage" is defined to encompass temporary, intermediate storage incidental to transmission as well as backup storage. The definition is not always easily applied.

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. 18 U.S.C. 2701(c). 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 in section 2702 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.

Public electronic communication service (ECS) providers to the public must keep confidential the content of any "communication while in electronic storage by that service." Public remote computer service (RCS) providers must keep confidential the content of "any communication which is carried or maintained on that service—(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." Both sets of providers must keep confidential any "record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any government entity."

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; (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.

SCA—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. Traditional exigent circumstances and a final general inconvenience justification form the grounds for delayed notification in either case: endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

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 its 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.

SCA—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, damages equal the loss and gain associated with the offense but not less than $1000. 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)

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."

The USA PATRIOT Act enlarged the coverage of sections 3121-3127 to include sender/addressee information relating to email and other forms of electronic communications.

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

PR/T&T—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. An order authorizing installation and use of a pen register or trap and trace device must: specify the person (if known) upon whose telephone line the device is to be installed, the person (if known) who is the subject of the criminal investigation, the telephone number, (if known) the location of the line to which the device is to be attached, and geographical range of the device, a description of the crime to which the investigation relates; upon request, direct carrier assistance pursuant to section 3124; terminate within 60 days, unless extended; involve a report of particulars of the order's execution in Internet cases; and impose necessary nondisclosure requirements.

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.

PRT&T—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 a separate federal private cause of action for victims of a pen register or trap and trace device violation. 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 decline to establish 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