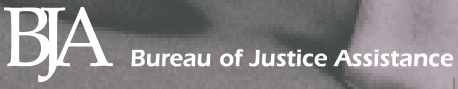
SPECIAL TOPICS SERIES

American
Prosecutors
Research Institute

The ECPA, ISPs & Obtaining E-mail:

A Primer for Local Prosecutors



Bureau of Justice Assistance

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
www.ndaa-apri.org

Thomas J. Charron
President

Roger Floren
Chief of Staff

Sean Morgan
Program Manager, White Collar Crime Program

Debra Whitcomb
Director, Grant Programs and Development

George Ross
Director, Grants Management

This document was produced under Grant No. 98LS-VX-0002 from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. This information is offered for educational purposes only and is not legal advice. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of the United States Department of Justice, the National District Attorneys Association, or the American Prosecutors Research Institute.

The American Prosecutors Research Institute is the nonprofit research, training and technical assistance affiliate of the National District Attorneys Association.

The ECPA, ISPs & Obtaining E-mail:

A Primer for Local Prosecutors

July 2005

Leonard Deutchman
Chief, Economic Crimes Unit
Philadelphia District Attorney's Office

Sean Morgan
White Collar Crime Program Manager
American Prosecutors Research Institute

Table of Contents

1 *Introduction*

3 *Why Should State and Local Prosecutors Care About Federal Law?*

9 *To Whom Does the ECPA Apply?*

11 *What Information Can Be Obtained Under the ECPA?*

13 *What Legal Process Can Be Used to Obtain Information Under the ECPA and to Request That ISPs Preserve That Information?*

23 *What Courts Can Issue Legal Process Under the ECPA and Who Can Execute That Process?*

25 *Conclusion*

INTRODUCTION

Many millions of e-mails are sent and received daily within the United States. The vast majority of these e-mails are sent for legitimate, legal purposes. However, e-mail has opened new vistas for criminals to perpetrate crimes like marketing fraud schemes through "phishing" or spam, to harass victims through cyber-stalking and to lure children and distribute child pornography. E-mail also has been used to commit traditional crimes, such as conspiracy to distribute narcotics and to plan violent crimes like robbery or murder.

As discussed in the companion APRI Special Report, *ABCs of E-mail*, e-mail is sent, received, and stored by Internet Service Providers (ISPs). To obtain evidence from an ISP, a law enforcement officer must, at a minimum, follow the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §2510 *et seq*., and, more particularly, the Stored Wire and Electronic Communications Act, 18 U.S.C. §§2701-2712 (referred to throughout collectively as "the federal law") within the ECPA. However, as was observed several years ago in a seminal case involving the ECPA,

> The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 *et seq*. is "famous (if not infamous) for its lack of clarity."

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F. 3d 457, 462 (5th Cir. 1994). Nevertheless, this infamous statute, which involves a "complex, often convoluted area of the law,"[1] governs an investigative task that has become increasingly necessary—obtaining e-mail, e-mail account information, and e-mail transactional records maintained by ISPs. Moreover, by using inconsistent, varying, and even misleading terminology, neither commentators nor the courts have assisted in clarifying the ECPA.

This APRI special report is intended to serve as a primer for the state or local prosecutor seeking to obtain e-mail information from ISPs. It is **not**

[1] *U.S. v. Smith*, 155 F. 3d 1051, 1055 (9th Cir. 1998).

legal advice and cannot substitute for reviewing the statutes or reading the small—but growing—body of case law that has dealt with the ECPA. In addition, because of the rapid pace of technological advances, e.g., the ability to send e-mail from cellular telephones or attach audio files to e-mail, authoritative legal guidance simply does not exist on some of the more esoteric issues involving the ECPA. Finally, state and local prosecutors should be aware that many states have enacted their own versions of the ECPA. As will be discussed in greater detail below, while the state versions may not be less restrictive, they certainly can be more restrictive in terms of how law enforcement obtains information relating to e-mail from ISPs.

This special report poses and discusses the five Ws of the ECPA, ISPs, and e-mail:

- **Why** should state and local prosecutors care about federal law?
- To **whom** does the ECPA apply?
- **What** information can be obtained under the ECPA?
- **What** legal process can be used to obtain information under the ECPA and request that ISPs preserve that information?
- **What** courts can issue legal process under the ECPA, and who can execute that process?

Why Should State and Local Prosecutors Care About Federal Law?

The question of why local prosecutors should care about federal law is one that at first seems complex, then simple, then complex. While it is not entirely clear that state and local prosecutors have to care, it is the more prudent course to do so. Furthermore, the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), made changes in the law that have actually empowered state and local prosecutors to **use the federal law in state court**. Finally, while a failure to follow the ECPA in obtaining e-mail information may not result in suppression of the evidence, it may result in civil liability for ECPA violators.

At first blush, there does not seem to be any reason for state and local prosecutors to care about the federal law. However, a review of the statutory history of the ECPA, in conjunction with Article VI of the Supremacy Clause of the United States Constitution, forces state and local prosecutors to care. Under the Supremacy Clause, when federal law and state law directly conflict, federal law controls. Title III of the Omnibus Crime Control Act of 1968, 18 U.S.C. §2510 *et seq.*, prohibits **all** oral, wire or electronic interception in the United States except under conditions set forth in Title III. Section 2511(1)(c)[2] authorizes law enforcement to conduct one-party consensual interceptions, while section 2511(1)(d) provides similar authorization to civilians, providing that interception is not performed to commit a criminal or tortuous act. Section 2516(1) authorizes federal law enforcement officers to perform non-consensual interceptions.

Section 2516(2) provides similar authority to state law enforcement officers, but only when state law authorizes such application:

[2] All statutory references are to title 18, United States Code, unless otherwise noted.

> The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving **the interception of wire, oral or electronic communications**, may apply to such judge for, and the judge may grant in conformity with section 2518[3] of this chapter and with the applicable State statute an order authorizing, or approving the **interception of wire, oral or electronic communications** . . . .

(Emphasis added). Under section 2516(2), state law must be co-extensive with federal law. It may, in addition, be more restrictive of electronic surveillance than is Title III, but it cannot be less.

Whether the co-extensiveness requirement applies to the ECPA is unclear. When Congress originally enacted the ECPA as part of the Omnibus Crime Control and Safe Streets Act of 1968, the ECPA's focus was on law enforcement's use of electronic surveillance, particularly wiretaps. For all intents and purposes, there was no such thing as electronic communications. In 1986, to address the advances in electronic communications technology Congress amended the ECPA to add the Stored Wire and Electronic Communications Act (SCA), 18 U.S.C. § 2701 *et seq*. The purpose of the SCA[4] was to update "existing federal wiretapping law to take into account new forms of electronic communications such as electronic mail, cellular telephones, and data transmission by providing such communications with protection against improper interception." 132 Congressional Record H. 4039 (June 23, 1986). This might suggest a legislative intent to treat **obtaining stored** electronic communications as Title III treats **intercepting transmission** of electronic communications. However, the text of Section 2516(2) makes clear that Title III applies solely to the **inter-**

[3] Section 2518 concerns the interception of wire, oral or electronic communications.

[4] While the statutory provisions regarding obtaining sent e-mail from ISPs (as opposed to intercepting e-mail during transmission) are located within SCA, most commentators refer to those provisions as the ECPA. To be consistent with those references, SCA will be referred to as the ECPA for the remainder of this article.

ception of communications, i.e., wiretaps. Further, because the SCA is a separate act with express provisions to cover the retrieval of communications in storage, it demonstrates that Congress meant to create an important distinction between interceptions and retrievals of electronic communications.

Congress added the SCA provisions to the ECPA because the Fourth Amendment does not accord an e-mail customer any right of privacy in communications stored by a third party (ISP). The right of privacy created by the SCA provisions of ECPA is, as with pen registers, wholly a creation of statute. *U.S. v. Miller*, 425 U.S. 435 (1976) held that a bank depositor had no Fourth Amendment right of privacy as to his bank records, and a whole line of cases has held consistently with *Miller*.[5] Indeed, the SCA provisions were adopted because users have no Fourth Amendment right of privacy in their stored communications, just as fed-

[5] The distinction between Title III's preemption of state law as to wiretaps and the inapplicability of federal pen register law to the states is not as clean as has been implied, but still holds. State law enforcement intersects with federal pen register law, 18 U.S.C. §§3127-27, in two ways. First, state law enforcement officers may obtain a pen register from a state court under federal law. *See* 18 U.S.C. §3123(a) (2) ("Upon an application…the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device…if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.") Second, state pen registers are required to restrict what they intercept to the telephone number at issue, and not to any "spillover" or message information. *See* 18 U.S.C. §3121(c) ("A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall restrict the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.") Interestingly, both intersections follow from the federal principle that, under *Smith v. Maryland*, supra, there are no Fourth Amendment implications to pen registers or trap and trace devices. Thus, under the first intersection, there should be no problem in allowing state law enforcement officers to obtain court orders. Moreover, as to the second intersection, the provision against intercepting the contents of any wire or electronic communication follows because, under federal law, there is no probable cause requirement to obtain a pen register order. Hence, even though there are federal rules regarding pen registers—which allow state law enforcement officers to get the numbers while concurrently restricting their use to prevent the interception of content information—these federal rules are consistent with the federal philosophy of giving protection only when the Fourth Amendment is implicated. As we shall see *infra*, this distinction is followed in the SCA provisions of the Electronic Communications Privacy Act, under which user and transactional information may be obtained with less than a showing of probable cause, while the content information of e-mails can be obtained principally through the issuance of a search warrant supported by probable cause.

eral banking laws giving account holders a right of privacy in their records were passed following *Miller.*[6]

Arguably, the ECPA distinguishes between interceptions covered by Title III, whose state analogs must conform to the dictates of Title III, and retrieval of stored communications, for which no federal standards are set. This argument makes sense in light of the privacy distinctions under federal law between wiretaps and stored communications. *Katz v. United States*, 389 U.S. 347 (1967) holds that the Fourth Amendment applies to wiretaps, while *Smith v. Maryland*, 442 U.S. 735 (1979) holds that there are no Fourth Amendment implications to the use of a pen register or trap and trace device. Accordingly, under federal law there is no probable cause, or even reasonable suspicion, requirement to obtain a pen register order; all that is needed is a certification that the order is in furtherance of a criminal investigation. *See* 18 U.S.C. §3122(b). Thus, for example, in *U.S. v. Miller*, 116 F.3d 641 (2d Cir. 1997), *cert. denied*, 524 U.S. 905 (1998), the court held that suppression would not lie in federal court for a state's violation of its own pen register laws when that violation concerned conditions that were more strict than those demanded by the federal law.

Because there is a difference between the Fourth Amendment rights protected under Title III and the statutorily-created rights found in the SCA provisions of the ECPA, and because the preemption language of Section 2516 so clearly applies solely to Title III, it can be argued that federal law regarding stored electronic communication (e-mail) does not preempt and control state law as does federal wiretap law. It is more difficult to interpret a situation where a state has set forth a complex statutory scheme dealing with the same issues as are addressed in ECPA: Does that evince an intent to "occupy the field," or a "reverse preemption" by the state? The federal courts have not hesitated to apply the federal ECPA to state actors. *See Ameritech Corp. v. McCann*, 297 F. 3d 582 (7th

[6] *See U.S. v. Steiger*, 318 F. 3d 1039 (11th Cir. 2003); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F. 3d 457 (5th Cir. 1994); *Garrity v. John Hancock State Life Insurance Company*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002); *U.S. v. Moriarity*, 1997 U.S. Dist. LEXIS 6678 (D. Mass. April 3, 1997); *Commonwealth v. Proetto*, 771 A.2d 823 (Pa. Super.), *aff'd*, 837 A.2d 1163 (2003); *State v. Evers,* 815 A. 2d 432 (N.J. 2003); *State v. Townsend*, 57 P. 3d 255 (Wash. 2002).

Cir. 2002) (district attorney held statutorily liable for payment of production fees under the ECPA); *Freedman v. America Online*, 303 F. Supp. 2d 121 (D. Conn. 2004) (local police officers violated the ECPA when they knowingly served an unsigned search warrant for e-mail); *Muskovich v. Crowell,* 1995 U.S. LEXIS 5899 (S.D. Ia. Mar. 21, 1995) (ECPA held to preempt state law claims for alleged ECPA violations).

In addition to the application of the ECPA to state and local law enforcement's obtaining of e-mail and e-mail related information, there are three other good reasons to follow federal law: (1) the PATRIOT Act empowers state courts with the authority to issue legal process for e-mail information; (2) failure to follow the ECPA may result in civil liability; and (3) ISPs generally will not turn over the information to law enforcement without ECPA compliance, since that could subject the ISP to civil liability.

The PATRIOT Act specifically amended Section 2703(d) of the ECPA to authorize state courts of "competent jurisdiction" to issue legal process under various sections of the ECPA unless "prohibited by the law of such State." Section 2711(3) defines a "court of competent jurisdiction" to issue legal process to include a court as defined by 18 U.S.C. §3127. Section 3127(2) (B) states "a court of general criminal jurisdiction of State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device." Thus, state and local prosecutors can use the ECPA to obtain, from their own state courts, legal process for collection of e-mail information and e-mail.

State and local prosecutors should also be aware that violations of the ECPA may subject them to civil or criminal liability. Section 2701(a) makes it a criminal offense to intentionally access "a facility through which an electronic communication is provided." Section 2707 provides that violators also may be subjected to civil liability. This civil liability is not merely theoretical. S*ee Konop v. Hawaiian Airlines*, 302 F. 3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F. 3d 457 (5th Cir. 1994); *Freedman v. America Online*, 303 F. Supp. 2d 121.

Finally, if state and local law enforcement do not comply with the ECPA, the ISPs do not have to turn over the e-mail or related information. In fact, if a provider of e-mail services (discussed more in detail, *infra*) does provide the information without the proper legal process, the provider could open itself to liability. The ISPs' concerns regarding ECPA liability are not misplaced. In *Freedman v. America Online*, 325 F. Supp. 2d 638 (E.D.Va. 2004), America Online was found to have violated the ECPA by providing subscriber information to local police officers who served an unsigned ECPA warrant. Interestingly, there is even a "safe haven" provision for the information provider at Section 2703(c), which states that if the information is provided pursuant to a subpoena, court order or search warrant, the provider may not be held liable.

Unlike Title III, the ECPA does not provide that evidence obtained in violation will be suppressed. *See U.S. v. Steiger*, 318 F. 3d 1039, 1051 (11th Cir. 2003); *U.S. v. Smith*, 155 F. 3d 1051 (9th Cir. 1998); *U.S. v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000); *U.S. v. Hambrick*, 55 F. Supp. 2d 504 (W.D.Va. 1999), *aff'd*, 225 F. 3d 656 (4th Cir. 2000); *U.S. v. Allen*, 53 M.J. 402 (Ct. App. A.F. 2000); *State v. Evers*, 815 A. 2d 432. However, be aware that a court may be tempted to graft a suppression remedy if it finds the conduct egregious or that law enforcement ignored the ECPA with seeming impunity.[7] Many federal courts, have, for example, suppressed wiretap evidence even where Title III expressly states that the errors found are not grounds for suppression. The point is, FOLLOW THE LAW—argue lack of suppression as a remedy only in that one-in-a-million situation where a mistake was made.

[7] *See McVeigh v. Cohen,* 983 F. Supp. 215 (D. D.C. 1998) (court found U.S. Navy investigator likely solicited a violation of the ECPA when the investigator obtained a sailor's online profile from America Online without legal process in an investigation relating to the Department of Defense's "don't ask, don't tell" policy; based on that determination the court found the online profile would likely be inadmissible in an injunctive proceeding brought by the sailor to enjoin his discharge from the U.S. Navy).

To Whom Does the ECPA Apply?

In terms of **seeking** information, ECPA applies to governmental entities. In terms of **who must provide information**, it applies to providers of electronic communications services (ECS) and remote computing services (RCS). Whether the entity requesting the information or possessing the information falls within these categories is important because it will determine the applicability of the ECPA and whether the provider may make voluntary disclosure.

Seeking Information

Under 18 U.S.C. §2703, a governmental entity can require disclosure of the content of wire or electronic communications that are in electronic storage, subscriber information, and electronic transmission or transactional information. The ECPA does not define governmental entity. The courts also have not defined governmental entity. An individual not employed or associated with governmental agencies can be considered a government agent if the individual has, under a totality of the circumstances, entered into an agency relationship with the governmental entity. *See U.S. v. Jarrett*, 338 F. 3d 339 (4th Cir. 2003), *cert. denied*, 124 S. Ct. 1457 (2004).

Providing Information

Section 2702 prohibits voluntary disclosure by a provider to the public of ECS or RCS of any records or information to a governmental entity unless done pursuant to the ECPA. Electronic communications service is defined at 18 U.S.C. §2510 as "any service which provides to users thereof the ability to send or receive wire or electronic communications . . . ." Remote computing service is defined at 18 U.S.C. §2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system . . . ."

An ISP is considered to be a provider both of ECS and of RCS and is thus prohibited from making voluntary disclosure. *See U.S. v. Kennedy*, 81

F. Supp. 2d 1103, 1111 (D. Kan. 2000). ISPs provide their e-mail account-holders with the ability to send and receive e-mail and typically, the ability to store sent or opened e-mail with the ISP's computer(s), typically referred to as a mail server(s). Indeed, the legislative history for ECPA identifies three types of typical ECS providers: "a telephone company; an electronic mail company; and a company providing remote computing services." *State Wide Photography Corp. v. Tokai Fin. Serv.*, 909 F. Supp. 137, 145 (S.D. N.Y. 1995).

A private provider of electronic communications, such as a corporation providing e-mail to its employees, also can be a provider of ECS and require that a governmental entity seeking information provide legal process in accordance with the ECPA. *See U.S. v. Mullins*, 992 F. 2d 1472 (9th Cir. 1993) (airline was an ECS where it provided an electronic travel reservation); *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) (city was an ECS that provided pager service to police officers). However, in the instance where the ECS does not provide electronic communications service to the public absent any state constitutional or statutory prohibition—the private provider of ECS may disclose voluntarily e-mail content and e-mail-related records. *See Dyer v. Northwest Airlines,* 334 F. Supp. 2d 1196 (D. N.D. 2004); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001); *Conner v. Tate*, 130 F. Supp. 2d (N.D. Ga. 2001); *Sherman & Co. v. Salton Maxim Housewares*, 94 F. Supp. 2d 817 (E.D. Mich. 2000); *Anderson Consulting v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998).

What Information Can Be Obtained Under the ECPA?

Section 2703 of the ECPA uses the terms "contents of wire or electronic communications" and "records concerning electronic service or remote computing service" to classify the types of information obtainable under the act. Commentators on the ECPA, as will be discussed *infra,* frequently use different terms: subscriber information, transactional information, and content. Subscriber information and transactional information are records and the e-mails themselves are considered content.[8] The category of information that the state or local enforcement officer is seeking is important because it greatly affects the next question regarding the legal process required to obtain the information.

Content of Wire or Electronic Communications

Content is defined by Section 2510 as "any information concerning the substance, purport, or meaning of" a communication. Obtaining e-mail from a provider of ECS or RCS when not done contemporaneously with transmission is not an intercept (and therefore not subject to Title III) because the e-mail is in electronic storage. *See Garrity v. John Hancock Mutual Life Insurance Company*, 2002 U.S. Dist. LEXIS 8343; *Commonwealth v. Proetto*, *supra* n.6. In *Frazier v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623 (E.D. Pa. 2001), the court held that acquisition of e-mail after it has been received is not an interception under federal law.

Records Concerning Electronic Communications Service or Remote Computing Service

Information considered to be records generally falls within two categories, subscriber information and transactional information. Section 2703(c)(2) provides that a governmental entity can obtain the following records "of a subscriber to or customer of" a provider of ECS or RCS:

- Name
- Address

[8] While the scope of this APRI special report is limited to a discussion of the ECPA and obtaining e-mail, it should be noted that the PATRIOT Act amended federal law so that voice-mail is now considered the content of stored wire communications. *See* 18 U.S.C. §2703 *passim*.

- Local and long distance connection records
- Session times and durations
- Length of service
- Types of service
- Telephone or instrument number
- Other subscriber's numbers or identity
- Temporarily assigned network addresses
- Service payment information, including any credit card or bank account number

This information is commonly referred to as subscriber information because of the reference "of a subscriber to or customer of such service" within Section 2703(c)(2). It is well established that subscribers do not have a reasonable expectation of privacy in the records described above. *See Guest v. Leis*, 255 F. 3d 325, 336 (6th Cir. 2001); *U.S. v. Kennedy*, 81 F. Supp. 2d at 1110; *U.S. v. Hambrick*, 55 F. Supp. 2d 504 (W.D.Va. 2000).

Section 2703(c)(1) covers the remaining category of information, which is essentially all information that is not content information as defined at Section 2510 and discussed in Section 2703(a) and (b) or subscriber information as listed in Section 2703(c)(2). Commentators commonly refer to this category as transactional information, although this term is not used or defined within the ECPA. Examples of transactional information include server logs, online profiles, and screen names.

What Legal Process Can Be Used to Obtain Information Under the ECPA and To Request That ISPs Preserve That Information?

Three types of legal process are available under the ECPA to obtain content and records information: ECPA warrants,[9] 2703(d) court orders, and subpoenas. In addition, depending upon the type of information sought, 2703(d) court orders and subpoenas may require notice to the subscriber.[10] Generally, the more personal the information sought, e.g., e-mail content, the higher the burden of proof for law enforcement to obtain the requisite legal process. The ECPA warrant must be supported by probable cause, the 2703(d) court order by "specific and articulable facts," and a subpoena typically by relevance.

The three types of legal process are also inclusive in a hierarchical manner, i.e., with an ECPA warrant, law enforcement can collect all types of information obtainable using a 2703(d) court order or subpoena. Likewise, with a 2703(d) court order, law enforcement can collect all types of information obtainable using a subpoena. Finally, the recent decision of *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) for those states within the jurisdiction of the U.S. Court of Appeals for the Ninth Circuit recently narrowed the available legal process to obtain e-mail content to an ECPA warrant as will be discussed *infra*.[11]

9 Commentators and the courts sometimes refer to the ECPA warrant as a search warrant. As will be discussed *infra*, the ECPA warrant is not a search warrant in the traditional sense, as a law enforcement officer does not have to be present at the execution of the ECPA warrant.

10 Notice can be delayed as will be discussed *infra*.

11 State and local law enforcement should also be aware that several large ISPs such as AOL, Yahoo, and Hotmail are currently providing e-mail content to law enforcement only pursuant to an ECPA warrant based on *Theofel*, *supra*, regardless of the location of the requesting governmental entity, service of the process, or maintenance of the records.

Content Information

As discussed on the previous page, content is "any information concerning the substance, purport, or meaning of" a communication. See 18 U.S.C. §2510. The ECPA makes two distinctions in the requisite legal process to obtain e-mail content: (1) whether the e-mail has been in storage with the ISP for 180 days or less; and (2) whether the e-mail has been opened or retrieved by the subscriber. The 180-day criterion is immediately discernible in the relevant statutory section (Section 2703); however, the second criterion (whether the e-mail is opened or unopened) is not evident. The key to deciphering the relevant statute, Section 2703, is its use of the terms, ECS or RCS.

As a practical matter, generally state and local law enforcement will want to obtain all e-mails relevant to an investigation, regardless of whether the e-mails are opened or unopened by the subscriber or of the stored age of the e-mails. Thus, the use of a 2703(d) court order or subpoena to obtain content in storage for more than 180 days or opened content is useful under the limited circumstances when state or local law enforcement: (1) are certain that only opened e-mails or e-mails in storage for more than 180 days are relevant; or (2) lack probable cause, but do have specific and articulable facts for a 2703(d) court order or can obtain a valid subpoena.

Unopened Content In Storage for 180 Days or Less

Under 18 U.S.C. §2703(a), state and local law enforcement must get a warrant to obtain unopened e-mail content in storage for 180 days or less from an ECS or RCS. Section 2703 authorizes issuance of a warrant "using the procedures described in the Federal Rules of Criminal Procedure" by either a federal court "with jurisdiction over the offense under investigation" or an "equivalent State warrant." When evidence is obtained in this manner, no notice is given to the subscriber. Moreover, the provider of ECS or RCS may be ordered not to disclose the ECPA warrant. *See* 18 U.S.C. §2705(b). Under federal law, grounds for ordering non-disclosure include reason to believe that disclosure will:

- endanger the life or physical safety of a person;
- result in flight from prosecution;
- result in destruction of or tampering with evidence;

- lead to witness intimidation; or
- otherwise seriously jeopardize an investigation or delay a trial.

Although there is no statutory reference to "unopened e-mail content" in Section 2703(a), its application to unopened e-mail is based upon the subsection's reference that it applies to obtaining content from an ECS. While an e-mail is unopened, a provider acts as an ECS for the subscriber by providing electronic communication; however, once the e-mail is opened, the provider furnishes RCS by providing electronic storage for the opened e-mail. A provider of RCS falls within the scope of the ECPA only when it acts as an RCS to the public. Thus, once the e-mail is opened, if the provider does not provide RCS to the public, legal process to obtain that e-mail is not governed by the ECPA at all; rather, it will be governed by the Fourth Amendment and any applicable state constitutional and statutory requirements.

Opened Content and Content In Storage for More than 180 Days

As discussed above, if the provider does not offer RCS to the public, then the ECPA does not apply for purposes of state and local law enforcement obtaining opened e-mail. However, if the provider is furnishing RCS to the public, Section 2703(b) of the ECPA governs state or local law enforcement's legal process to obtain opened e-mail content using:

- an ECPA warrant;[12]
- a 2703(d) court order with prior notice to the subscriber;[13] or
- a federal or state administrative, grand jury, or trial subpoena with prior notice to the subscriber.

The ECPA treats unopened e-mail in storage for more than 180 days the same as opened e-mail. Section 2703(a) specifically provides, in relevant part, that:

> A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one

[12] An ECPA warrant is the **only** legal process that does not require notice to the subscriber to obtain content.

[13] Obtaining 2703(d) court orders will be discussed in more detail *infra*.

hundred and eighty days by the means available under subsection (b) of this section.

Notice

Section 2705 provides that notice can be delayed upon written certification of a supervisory official[14] for a subpoena or application for a 2703(d) court order when there is reason to believe that disclosure will:

- endanger the life or physical safety of a person;
- result in flight from prosecution;
- result in destruction of or tampering with evidence;
- lead to witness intimidation; or
- otherwise jeopardize an investigation or delay a trial.

Notification delays can be for as long as 90 days, and can be extended for additional 90-day periods by subsequent certifications or applications. Upon expiration of the delay period, the state or local law enforcement agency obtaining the information must provide notice to the subscriber in accordance with Section 2705(a)(5), which requires service of the 2703(d) court order or subpoena on the subscriber by registered or first class mail and notice that:

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certifica-

[14] "Supervisory official" is defined at Section 2705(a)(6) as:

the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

tion or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

In addition, as with an ECPA warrant, state or local law enforcement can request a court order that the ISP not disclose the legal process or compliance to the subscriber. *See* 18 U.S.C. §2705(b); *In re Application of the United States,* 157 F. Supp. 2d 286 (S.D. N.Y. 2001). However, be aware that to obtain the information from electronic storage, an ISP may have to close the subscriber's account or alter the e-mail status, which could result in alerting the subscriber.

Theofel States

The court's decision in *Theofel v. Farey-Jones,* 359 F.3d 1066 (9th Cir. 2003) has had the net effect of limiting the legal process available to obtain e-mail content to an ECPA warrant for states within its jurisdiction,[15] regardless of whether the e-mail had been opened or in storage for more than 180 days. The court reached that conclusion based on an arcane fact pattern involving:

- a civil suit;
- one litigant obtaining an invalid subpoena for the other litigant's e-mail;
- the ISP providing some of the requested e-mail content;
- resulting in a subsequent ECPA civil action by the litigant whose e-mail was obtained.

In *Theofel*, the court based its decision on the voluntary disclosure prohibition regarding content in Section 2702 (a) (1) and (2), which states that a provider of ECS or RCS to the public "shall not knowingly divulge . . . the contents of any communication . . . ." The court concluded that the Section 2702 prohibition governing divulgement of e-mail applied regardless of whether the e-mail was opened and that a subscriber's opening of e-mail did not affect the ISP's status as an ECS. Therefore, because a provider to the public of ECS or RCS can only disclose e-mail contents

[15] The following states and territories are within the jurisdiction of the U.S. Court of Appeals for the Ninth Circuit and subject to *Theofel:* Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Washington, Guam, and the Northern Mariana Islands.

and records under the exceptions enumerated in Section 2702(b), the subject ISP's disclosure of e-mail content pursuant to an invalid subpoena violated the ECPA.[16]

The bottom line of the *Theofel* decision: For state and local law enforcement or providers to the public of ECS or RCS located within the jurisdiction of the U.S. Court of Appeals for the Ninth Circuit, e-mail content can only be obtained using an ECPA warrant. In addition, some ISPs will only provide content pursuant to an ECPA warrant, regardless of their location or the law enforcement agency's location.

Records

Under Section 2703(c), all records, transactional and subscriber, can be obtained using any of the following processes:
- an ECPA warrant;
- a 2703(d) court order;
- consent of the subscriber; or
- a formal written request to the ECS/RCS that the information sought is relevant to a law enforcement investigation of telemarketing fraud.

In addition, a federal or state administrative, grand jury, or trial subpoena can be used to obtain subscriber records **only.** As discussed previously, subscriber records are:
- Name
- Address
- Local and long distance connection records
- Session times and durations
- Length of service
- Types of service
- Telephone or instrument number
- Other subscriber's numbers or identity
- Temporarily assigned network addresses
- Service payment information, including any credit card or bank account number

Further, state or local law enforcement can request a court order that the

[16] An exception to the Section 2702 disclosure prohibition includes the issuance of valid legal process as provided in Section 2703.

ISP not disclose the legal process or compliance to the subscriber. *See* 18 U.S.C. §2705(b).

2703(d) Court Order

Section 2703(d) authorizes "any court that is a court of competent jurisdiction," which includes state courts unless "prohibited by the law of such state,"[17] to issue an order compelling a provider to provide records, that is, all non-content information.

To obtain a 2703(d) court order, the applicant must provide "specific and articulable facts" that show:

- reasonable grounds to believe that the content of the electronic communications or requested records…
- are relevant and material to an ongoing investigation.

Typically, the application for a 2703(d) court order provided to the court will contain:

- an application for the 2703(d) court order;
- a statement of specific and articulable facts in support of reasonable grounds;
- a draft 2703(d) court order; and
- a draft sealing order of one page.

Voluntary Disclosure

Section 2702(a) permits disclosure of content by a public provider of ECS/RCS:

- to the addressee recipient or addressee recipient's agent;
- with consent from the originator, addressee recipient, or subscriber for an RCS;
- in accordance with legal process pursuant to the ECPA;
- to any person whose facility was used to forward the content;
- as necessary to protect the provider or provision of service;
- to law enforcement if the contents were inadvertently obtained and appear to pertain to the commission of a crime;

[17] It is unclear what is required for a state to "prohibit" its courts from issuing Section 2703(d) orders. An express statutory prohibition passed after the enactment of the USA PATRIOT Act should suffice.

- to a governmental entity "if the provider in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay …."

Section 2702(b) permits disclosure of records of a public provider of ECS/RCS:
- in accordance with legal process pursuant to the ECPA;
- with consent of the subscriber;
- as necessary to protect the provider or provision of service;
- to a governmental entity "if the provider in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay ….;"
- to the National Center for Missing and Exploited Children, under certain circumstances; and
- to any person other than a governmental entity.

What is extremely significant in Section 2702 is that it limits the prohibitions of voluntary disclosure only to providers **to the public** of ECS and RCS**.** Therefore, non-public providers of e-mail services may voluntarily disclose any content or records to law enforcement; however, if the private provider will not make voluntary disclosure, then the ECPA and any applicable state constitutional or statutory requirements will dictate the requisite legal process for law enforcement to obtain the e-mail records or content.

Preservation of Content & Records

Records and/or content should be requested **as soon as possible**. Retention periods for subscriber and transactional records and e-mail content records vary greatly among ISPs. Moreover, there are no statutorily mandated or industry guidelines regarding preservation of this information prior to request from law enforcement. Indeed, it is not unusual for ISPs to dispose of e-mail information and content after only days, even hours. To ensure that records and content will be preserved pending service of legal process, Section 2703(f) provides that upon request from a governmental entity, a provider of ECS or RCS shall retain all records or evidence for up to 90 days pending issuance of legal process. The ini-

tial 90-day preservation period can be extended up to an additional 90 days with a supplemental request. Moreover, law enforcement can require the ISP to make a backup copy of the requested information. *See* 18 U.S.C. §2704.

Production Costs

Section 2706 provides that a governmental entity "shall pay to the person or entity assembling or providing such information a fee for reimbursement . . . ." Such costs can include costs "due to necessary disruption of normal operations . . . ." The costs are to be mutually agreed upon, or in the absence of agreement determined by the court that issued the legal process to obtain the records or content. Moreover, the cost-reimbursement provisions of the ECPA supersede any immunity for cost reimbursement provided by state sovereignty. *See Ameritech Corp. v. McCann*, 297 F. 3d 582 (7th Cir. 2002).

What Courts Can Issue Legal Process Under the ECPA, and Who Can Execute That Process?

Regarding ECPA warrants, Section 2703(a), (b)(1)(A), and (c)(1)(A) specifically provide that content and records can be obtained "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant." Thus, a state court empowered to issue a search warrant is endowed with the power to issue an ECPA warrant. However, unless the place of service for the ECPA warrant is located within the same state as the issuing judge, or in California, Minnesota, or Florida,[18] the law enforcement agency will need to obtain an ECPA warrant from a judge with appropriate authority in the same state as the ECS/RCS. In that instance, the law enforcement agency seeking the records or content will need to draft an affidavit, provide it to a law enforcement agency within the same jurisdiction as the ECS/RCS, and have that agency obtain an ECPA warrant from a "court of competent jurisdiction."

The PATRIOT Act specifically amended the ECPA at Section 2703(d) to authorize state courts of "competent jurisdiction" to issue 2703(d) court orders and subpoenas pursuant to the ECPA unless "prohibited by the law of such State." Section 2711(3) defines the term "court of competent jurisdiction" as including a court as that term is defined at 18 U.S.C. §3127. Section 3127(2) (B) defines court as including "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device."

[18] California, Minnesota, and Florida have full faith-and-credit statutes that give out-of-state ECPA warrants full faith and credit in their jurisdictions; therefore, for providers of ECS or RCS located in those states, an ECPA warrant issued by a court of competent jurisdiction from the law enforcement agency's home state should suffice.

Other than the requirement that the issuing court be of competent jurisdiction, as discussed above, the ECPA does not restrict the local issuance of 2703(d) court orders or subpoenas with service on out-of-state ISPs.[19] If out-of-state service is challenged by the ISP, the law enforcement agency may have to invoke its state's long-arm witness statute or version of the Uniform Act to Compel Attendance of Witnesses (commonly referred to as the "multi-state compact").

Under Section 2703(g), a law enforcement officer does **not** have to be present when an ECPA warrant is served. This makes sense, because an ECPA warrant is, for all intents and purposes, simply a subpoena *duces tecum*; the sole reason that a warrant is required under ECPA is because of the quantum of proof needed to obtain it—probable cause—as opposed to the "reasonable grounds" quantum to obtain a 2703(d) court order. In *U.S. v. Bach*, 310 F. 3d 1063 (8th Cir. 2002), the U.S. Court of Appeals for the Eighth Circuit, interpreting Minnesota law requiring that a law enforcement officer execute all search warrants, held that suppression did not lie where an ECPA warrant was issued in Minnesota but served in California without a local law enforcement officer present.

[19] However, a state's laws may affect the legality of out-of-state service. Some states, most notably New York, actually prohibit their courts from issuing legal process under the ECPA for service out-of-state.

CONCLUSION

E-mail usage for professional and personal purposes is as common as telephoning. Unfortunately, e-mail is also used to conduct or further criminal acts, and the necessity for law enforcement to obtain e-mail records or content in a criminal investigation or case is growing concomitantly. While obtaining e-mail records and content from providers of e-mail services ordinarily will not implicate the Fourth Amendment, it may implicate the SCA provisions of the ECPA. In addition, although violation of the ECPA by state and local law enforcement in obtaining e-mail may not result in suppression of the records or content obtained, it could result in civil or even criminal liability.

The threshold questions in assessing ECPA applicability are:
- Does the provider offer e-mail services to the public?
- Is the law enforcement agency seeking e-mail content?

If the provider offers e-mail services to the public, then it is almost certainly a provider of ECS or RCS and obtaining records or content will be governed by the ECPA. If the provider does not offer e-mail services to the public, it can require legal process pursuant to the ECPA for records and unopened e-mail content; however, the non-public provider may also make voluntary disclosure. With few exceptions, ISPs will fall within the category of public provider. An ECPA warrant will be necessary in the vast majority of investigations because it is only legal process to obtain unopened content. Only in those limited instances where the law enforcement agency lacks probable cause to obtain opened content, or seeks to obtain opened e-mail content or e-mail content in storage for more than 180 days, will the law enforcement agency have to engage in the more complex analysis of whether a 2703(d) court order or subpoena may be used.[20]

[20] Moreover, even if a law enforcement agency wants to obtain only opened e-mail content or e-mail content in storage for more than 180 days, the law enforcement agency can still use an ECPA warrant so long as there is probable cause.

To obtain records, the ECPA will apply if the provider furnishes ECS or RCS. Subscriber records can be obtained using an ECPA warrant, 2703(d) court order, or subpoena. If other types of records are sought, then generally only an ECPA warrant or 2703(d) court order will do. The private or non-public provider of e-mail services also may voluntarily disclose records or content to law enforcement.

Another concern that should be foremost in obtaining e-mail records and content is preservation. The use of preservation letters is very important, as there are no legal requirements or industry guidelines that mandate ISPs to retain records or content for any discrete period of time. Indeed, maintenance of such information costs money, and it generally does not serve the business interests of the ISP to preserve e-mail records and content any longer than necessary to serve the customer and obtain payment.

It also should be noted that several amendments to the ECPA wrought by the PATRIOT Act will expire on December 31, 2005, unless extended. Most significantly for state and local prosecutors will be the subtraction of voice-mail from the SCA provisions of the ECPA, and of state court's authority to issue 2703(d) court orders.

Finally, in obtaining e-mail content and records, law enforcement should remain aware that ECPA legal process is not prospective. It applies only to information that is in the possession of the provider at the time of service—not future information. To obtain future information or prospective preservation, a wiretap order will generally be needed.

The ECPA is a complex statutory scheme that even the courts have had difficulty in divining. However, with some forethought, legal analysis and coordination with the ISP, state and local law enforcement can obtain the appropriate legal process to receive information that can be critical to successful investigation and case resolution.

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, Virginia 22314
Phone: (703) 549-4253
Fax: (703) 836-3195
http://www.ndaa-apri.org

APRI