Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice

July 2002

[EXCERPT]

D. Compelled Disclosure Under ECPA [The Electronic Communications Privacy Act]

18 U.S.C. § 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information such as account records and basic subscriber information.

Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms, in ascending order of required threshold showing, are as follows:

1) Subpoena;

2) Subpoena with prior notice to the subscriber or customer;

3) § 2703(d) court order;

4) § 2703(d) court order with prior notice to the subscriber or customer; and

5) Search warrant.

One feature of the compelled disclosure provisions of ECPA is that greater process generally includes access to information that can be obtained with lesser process. Thus, a § 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a § 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified, both because it can authorize a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the statute. Note, however, the notice requirement must be considered as a separate burden under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a § 2703(d) order without subscriber notice. (One small category of information can be compelled under ECPA without a subpoena. When investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing. See 18 U.S.C. § 2703(c)(1)(D).)

1. Subpoena

Investigators can subpoena basic subscriber information.

ECPA permits the government to compel two kinds of information using a subpoena. First, the government may compel the disclosure of the basic subscriber information (discussed above in section C.1) listed in 18 U.S.C. § 2703(c)(2):

(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

18 U.S.C. § 2703(c)(2).

Agents can also use a subpoena to obtain information that is outside the scope of ECPA. The hypothetical e-mail exchange between Jane and Joe discussed in Part B of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened e-mail on Good Company's server. See Part B, supra. Accordingly, § 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling Good Company to divulge the communication just as they would if ECPA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by ECPA, and may be obtained using a subpoena according to the same rationale. Cf. Organizacion JD Ltda. v. United States Department of Justice, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in ECPA).

The legal threshold for issuing a subpoena is low. See United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950). Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to Fed. R. Crim. P. 6(e). Types of subpoenas other than federal grand jury subpoenas may be used to obtain disclosure pursuant to 18 U.S.C. § 2703(c)(2): any federal or state grand jury or trial subpoena will suffice, as will an administrative subpoena authorized by a federal or state statute. See 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by § 6(a)(4) of the Inspector General Act may be used. See 5 U.S.C. app. However, at least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. See FTC v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000) (holding that pre-trial discovery subpoena did not fall within the meaning of "trial subpoena"). Sample subpoena language appears in Appendix E.

2. Subpoena with Prior Notice to the Subscriber or Customer

Investigators can subpoena opened e-mail from a provider if they comply with the notice provisions of §§ 2703(b)(1)(B) and 2705.

Agents who obtain a subpoena, and either give prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a), may obtain:

1) everything that can be obtained using a subpoena without notice;

2) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2); and

3) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

As a practical matter, this means that agents can obtain opened e-mail (and other stored electronic or wire[(15)] communications in "electronic storage" more than 180 days) using a subpoena, so long as they comply with ECPA's notice provisions. See H.R. Rep. No. 99-647, at 64-65 (1986).

The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. See 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) and § 2705(a)(4) permit notice to be delayed for ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. See § 2705(a)(2) (defining "adverse result"); § 2705(a)(6) (defining "supervisory official"). This provision of ECPA provides a permissible way for agents to delay notice when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. Upon expiration of the delayed notice period,[(16)] the statute requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5).

ECPA's provision allowing for obtaining opened e-mail using a subpoena combined with prior notice to the subscriber appears to derive from Supreme Court case law interpreting the Fourth and Fifth Amendments. See Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping § 26:9, at 26-12 (2d ed. 1995). When an individual gives paper documents to a third-party such as an accountant, the government may subpoena the paper documents from the third party without running afoul of either the Fourth or Fifth Amendment. See generally United States v. Couch, 409 U.S. 322 (1973) (rejecting Fourth and Fifth Amendment challenges to subpoena served on defendant's accountant for the accountant's business records stored with the accountant). In allowing the government to subpoena opened e-mail, "Congress seems to have concluded that by 'renting' computer storage space with a remote computing service, a customer places himself in the same situation as one who gives business records to an accountant or attorney." Fishman & McKenna, §26:9, at 26-13.

3. Section 2703(d) Order

Agents need a § 2703(d) court order to obtain most account logs and most transactional records.

Agents who obtain a court order under 18 U.S.C. § 2703(d) may obtain:

- 1) anything that can be obtained using a subpoena without notice; and
- 2) all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court or equivalent state court judge. See 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order, known as an "articulable facts" court order or simply a "d" order,

the governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Id.

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. See United States v. Kennedy, 81 F. Supp. 2d 1103, 1109-11 (D. Kan. 2000) (concluding that a conclusory application for a § 2703(d) order "did not meet the requirements of the statute."). The House Report accompanying the 1994 amendment to § 2703(d) included the following analysis:

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 102-827, at 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511 (quoted in full in Kennedy, 81 F. Supp. 2d at 1109 n.8). As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. A sample § 2703(d) application and order appears in Appendix B.

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. ECPA permits a judge to enter § 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. See 18 U.S.C. § 2703(d) (stating that "any court that is a court of competent jurisdiction" may issue a § 2703(d) order) (emphasis added); 18 U.S.C. § 2711(3) (stating that "'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographical limitation")[(17)]; 18 U.S.C. § 3127(2) (defining "court of competent jurisdiction").

Section 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B) (defining "court of competent jurisdiction" to include "a court of general criminal jurisdiction of a

State authorized by the law of the State to enter orders authorizing the use of a pen register or trap and trace device"). However, the statute does not confer extraterritorial effect on § 2703(d) orders issued by state courts. See 18 U.S.C. §§ 2711(3).

4. § 2703(d) Order with Prior Notice to the Subscriber or Customer

Investigators can obtain everything in an account except for unopened e-mail or voicemail stored with a provider for 180 days or less using a § 2703(d) court order that complies with the notice provisions of § 2705.

Agents who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

- 1) everything that can be obtained using a § 2703(d) court order without notice;
- 2) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2); and
- 3) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

As a practical matter, this means that the government can obtain the full contents of a subscriber's account except unopened e-mail and voicemail (which has been in "electronic storage" 180 days or less) using a § 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B).[(18)]

As an alternative to giving prior notice, agents can obtain an order delaying notice for up to ninety days when notice would seriously jeopardize the investigation. See 18 U.S.C. § 2705(a). In such cases, agents generally will obtain this order by including an appropriate request in the agents' 2703(d) application and proposed order; sample language appears in Appendix B. Agents may also apply to the court for extensions of the delay. See 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(4). The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. See Part D.2., supra. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(2). Importantly, the applicant must satisfy this standard anew every time the applicant seeks an extension of the delayed notice.

5. Search Warrant

Investigators can obtain the full contents of an account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant may obtain:

- 1) everything that can be obtained using a § 2703(d) court order with notice; and
- 2) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a).

- In other words, agents can obtain every record and all of the contents of an account by obtaining a search warrant based on probable cause pursuant to Fed. R. Crim. P. 41.[21] The search warrant can then be served on the service provider and compels the provider to divulge to law enforcement the information described in the search warrant. Notably, obtaining a search warrant obviates the need to give notice to the subscriber. See 18 U.S.C. § 2703(b)(1)(A). Moreover, because the warrant is issued by a neutral magistrate based on probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

Although most search warrants obtained under Rule 41 are limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703(a) may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district.[22] 18 U.S.C. § 2703(a). (State courts may also issue warrants under § 2703(a), but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. See id.) Otherwise, as a practical matter, § 2703(a) search warrants are obtained just like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41. See 18 U.S.C. § 2703(a). Once a magistrate judge signs the warrant, however, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material described in the warrant.

One district court recently held unconstitutional the practice of having service providers produce the materials specified in a search warrant. See United States v. Bach, 2001 WL 1690055 (D. Minn. Dec. 14, 2001). In Bach, state law enforcement officials obtained a search warrant under state law for information regarding a Yahoo email account and faxed the warrant to Yahoo, which produced the appropriate documents. The district court suppressed the results of the search as a Fourth Amendment violation. The court held that the Fourth Amendment mandates the protections codified in 18 U.S.C. § 3105, which requires that a law enforcement officer be present and act in the execution of a search warrant. According to the court, "section 2703 is not an exception to and does not provide an alternative mode of execution from section 3105," so federal law enforcement officials are mandated by statute to comply with § 3105 when executing a search warrant under 2703(a). The court held that even in the absence of a statutory mandate, the Fourth Amendment requires a law enforcement officer to be present and act in the execution of any search warrant, including a warrant issued under 2703(a).

The government has appealed the Bach decision. The government's brief points out that, leaving aside Bach's questionable Fourth Amendment jurisprudence and the inappropriateness of the suppression remedy, ECPA makes clear Congress's intent to authorize the use of § 2703 search warrants for subscriber content as a form of compulsory process directed to third-party network providers - not as a traditional search warrant. See, e.g., 18 U.S.C. §§ 2702(b)(2), (c)(1) (stating explicitly that a provider may disclose customer records in response to § 2703 process). Furthermore, even if 18 U.S.C. § 3105 were applicable to warrants served pursuant to ECPA, § 3105 does not require the presence of law enforcement when service providers collect and produce information pursuant to a search warrant because the problems associated with private exercise of search and seizure powers are not implicated when service providers collect and produce information in response to a warrant. See In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, 616 F.2d 1122, 1130 (9th Cir. 1980); In re Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, 610 F.2d 1148, 1154 (3rd Cir. 1979). Moreover, practically speaking, requiring the presence of law enforcement at the execution of these search warrants would prove extremely burdensome, as searches can prove time consuming, and ISPs maintain account information in a variety of locations. Also, it is difficult to imagine how a law enforcement officer could play a useful role in a service provider's actual retrieval of the specified records.

Nevertheless, in the interest of caution, until the issues raised in Bach are ultimately resolved, law enforcement officials preparing a warrant pursuant to § 2703 are advised to request in the search warrant application that the magistrate expressly permit faxing the warrant to the ISP and executing the warrant without the officer present. For draft language or other information and guidance regarding Bach, contact the Computer Crime and Intellectual Property Section at (202) 514-1026.

E. Voluntary Disclosure

Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. ECPA imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

The voluntary disclosure provisions of ECPA appear in 18 U.S.C. § 2702. These provisions govern when a provider of RCS or ECS can disclose contents and other information voluntarily, both to the government and non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, agents must rely on compelled disclosure provisions and obtain the appropriate legal orders.

When considering whether a provider of RCS or ECS can disclose contents or records, the first question agents must ask is whether the relevant service offered by the provider is available "to the public." If the provider does not provide the applicable service "to the public," then ECPA does not place any restrictions on disclosure. See 18 U.S.C. § 2702(a). For example, in Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed to the *Wall Street Journal* e-mails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated ECPA. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public:

[G]iving Andersen access to [UOP's] e-mail system is not equivalent to providing e-mail to the public. Andersen was hired by UOP to do a project and as such, was given access to UOP's e-mail system similar to UOP employees. Andersen was not any member of the community at large, but a hired contractor.

Id. at 1043. Because UOP did not provide services to the public, ECPA did not prohibit disclosure of contents belonging to UOP's "subscribers."

If the services offered by the provider *are* available to the public, then ECPA forbids both the disclosure of contents to any third party and the disclosure of other records *to any governmental entity*, unless a statutory exception applies.[(21)] Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

ECPA provides for the voluntary disclosure of contents when:

1) the disclosure "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," § 2702(b)(5);

2) the disclosure is made "to a law enforcement agency . . . if the contents . . . were inadvertently obtained by the service provider . . .[and] appear to pertain to the commission of a crime," § 2702(b)(6)(A);

3) the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay," § 2702(b)(6)(C);

4) the Child Protection and Sexual Predator Punishment Act of 1998, 42 U.S.C. § 13032, mandates the disclosure, 18 U.S.C. § 2702(b)(6)(B); or

5) the disclosure is made to the intended recipient of the communication, with the consent of the intended recipient or sender, to a forwarding address, or pursuant to a court order or legal process. § 2702(b)(1)-(4).

ECPA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:[(22)]

1) the disclosure "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," § 2702(c)(3);

2) the provider "reasonably believes that an emergency involving immediate danger of death of serious physical injury to any person" justifies disclosure, § 2702(c)(4); or

3) the disclosure is made with the consent of the intended recipient, or pursuant to a court order or legal process § 2702(c)(1)-(2).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and service providers outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

F. Quick Reference Guide

Voluntary Disclosure Allowed?		**Mechanisms to Compel Disclosure**		
Public Provider	Non-Public Provider		Public Provider	Non-Public Provider
Basic subscriber, session, and billing information	Not to government, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]
Other transactional and account records	Not to government, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	2703(d) order or search warrant [§ 2703(c)(1)]	2703(d) order or search warrant [§ 2703(c)(1)]
Accessed communications (opened e-mail and voice mail) left with provider and other stored files	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	Subpoena; ECPA doesn't apply [§ 2711(2)]
Unretrieved communication, including e-mail and voice mail (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]
Unretrieved communication, including e-mail and voice mail (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]