Electronic Communications

Obtaining Email, Voicemail, and Text Messages

SHAREE1013: Jerry I am scared.
Jlc1006: Me too—don't try to hide it.
SHAREE1013: Jerry, don't look at him, don't talk to him.
Jlc1006: Don't worry.
SHAREE1013: Just do it and get the hell out of there.

Emails from Sharee Miller and her boyfriend as they plot the murder of Miller's husband. *Miller* v. *Stovall* (2008) 573 F.Supp.2d 964.

Email, voicemail, and texting have changed the way almost everyone communicates these days, including co-conspirators. For example, a British Airways employee who had been recruited to help plant a bomb on an airliner received the following email from his recruiter, Anwar al Awlaki: "Our highest priority is the U.S. Anything there, even if on a smaller scale compared to what we may do in the U.K. would be our choice. So the question is: is it possible to get a package or a person with a package on board a flight heading to the U.S.?" (Anwar never got a satisfactory answer to his question; he was killed in a CIA-led drone strike.)

In another case, a man named Ron Williams was about to murder his wife in their home in Florida when he inadvertently hit the speed dial button on his cell phone which called the house. The call went to voicemail which captured the terrifying sounds of his wife being stabbed to death. Investigators obtained a copy of the voicemail, and prosecutors played it to the jury in Williams' murder trial. To no one's surprise, he was convicted.

As Ron Williams, Anwar al Awlaki, Sharee Miller and countless other felons have learned, electronic communications technology is as useful to criminal investigators as it is to the criminals themselves. But while the technology is helpful, the law that regulates it is not. In fact, courts and commentators have aptly described it as "dense and confusing,"[1] and "a complex, often convoluted area of the law."[2] As a result, officers, prosecutors, and even judges have often been unsure of the standards and procedures by which copies of these types of communications can be obtained from service providers.

Fortunately, the law in this area has developed to the point that it is now fairly intelligible. For this reason, we decided to revisit the subject and bring our readers up to date on how the courts have been deciding cases in which email, voicemail, and text messages were admitted as evidence in criminal trials. But to really grasp this subject, it is necessary to understand the framework upon which this area of the law has been built. So that is where we will start.

The Stored Communications Act

In the past, there were essentially only two ways for people to communicate if they were not within shouting distance: telephone and mail. Consequently, the rules were fairly simple: To intercept telephone conversations, officers needed a wiretap order; to read someone's mail, they needed a search warrant.[3]

In the 1980s, however, dramatic developments in computer and telecommunications technologies provided the public with much faster and more convenient ways to communicate, most notably email and voicemail, and later the cell phones and text messaging. As the Sixth Circuit observed last year:

> Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become so pervasive that some persons may consider it to be an essential means or necessary instrument for self-expression, even self-identification.[4]

In a strange twist of fate, however, it turned out that the manner in which this new technology transmits messages rendered them "not private" under the Fourth Amendment. This was because the

[1] Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1208.
[2] *U.S.* v. *Smith* (9th Cir. 1998) 155 F.3d 1051, 1055.
[3] See *Ex parte Jackson* (1877) 96 U.S. 727, 728 ["Whilst in the mail, [letters] can only be opened and examined under like warrant"].
[4] *U.S.* v. *Warshak* (6th Cir. 2011) 631 F.3d 266, 286 [quoting from *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619, 2631]].

Supreme Court has consistently ruled that, under the Fourth Amendment, a person cannot ordinarily expect privacy in information that he has transmitted through an intermediary.[5] And that is exactly what happens when a person sends an electronic communication because the message must be copied and stored along the way (at least temporarily) on equipment that is owned and controlled by the service provider. Thus, criminal investigators could (at least theoretically) obtain copies of electronic communications from providers by simply asking.

In reality, however, virtually everyone who communicates by email, voicemail, or texting expects that their messages will be private, especially since there is no reason for the providers or their employees to read them.[6] While it is almost certain that the Supreme Court will someday re-examine its rulings on the issue and address this discord, Congress acted first, having decided that if the Fourth Amendment did not protect the privacy of these forms of communications, it would write a law that did. The result was the Stored Communications Act of 1986 (SCA).[7]

As Congress was writing the SCA, one of the most important decisions it needed to make was whether the rules covering the acquisition of electronic communications by law enforcement would be subject to the same strict requirements that govern the interception of phone conversations and the reading of mail, or whether they should be subject to less restrictive standards. Ultimately, it decided to impose less restrictive standards, mainly because people who communicate in this manner know that their messages are stored and are easily copied and, thus, they have a somewhat reduced expectation that their messages will remain private.

While Congress made its intent on this issue clear, the bulk of the SCA was disorganized and poorly written. As Georgetown law professor Orin Kerr pointed out, judges, legislators, and even legal scholars "have had a very hard time making sense of the SCA."[8] To make matters worse, the courts have been unable or unwilling to clarify the various issues and provide the kinds of guidance that investigators desperately need. In fact, in 2010 when the United States Supreme Court had an opportunity to provide some direction, it not only ducked the issue, it advised the lower courts to do the same. Here are the Court's words: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[9] And yet, the role of this technology will not become "clear" for decades (if not centuries) because it is constantly changing and expanding. As the Sixth Circuit warned in *United States* v. *Warshak*, "[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[10]

So, given the failure of Congress to write a comprehensible explanation of the law and the Supreme Court's suggestion that the lower courts remain above the fray for a while, and also given the scarcity of published criminal cases in this area,[11] it is no wonder that officers, prosecutors, and judges might seem perplexed.

Nevertheless, as noted earlier, the fundamental principles and basic requirements of the law have become much more understandable lately, thanks mainly to a few judges and legal commentators who have attempted to penetrate this "dense and confusing" subject and make sense of it.

---

[5] See *Smith* v. *Maryland* (1979) 442 U.S. 735, 743; *United States* v. *Miller:* (1976) 425 U.S. 435, 443.

[6] **NOTE**: One indication that the Court may so rule is found in its decision in *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]. In *Quon*, the Court could have simply resolved the issue by reaffirming its rule that people cannot reasonably expect privacy in stored text messages. Instead, it assumed for the sake of argument that stored text messages were, in fact, private under the Fourth Amendment. Also see *Wilson* v. *Moreau* (D.R.I. 2006) 440 F.Supp.2d 81, 108 ["the Court holds that Donald P. had a reasonable expectation of privacy in his personal Yahoo e-mail account"].

[7] 18 U.S.C. 2701 *et seq*.

[8] Orin S. Kerr, "A User's Guide to the Stored Communications Act," (2004) 72 Geo. Wash. L. Rev. 1208.

[9] *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]. Also see *Rehberg* v. *Paulk* (11th Cir. 2010) 611 F.3d 828, 844 ["The Supreme Court's most-recent precedent *[Quon]* shows a marked lack of clarity in what privacy expectations as to content of electronic communications are reasonable."].

[10] (6th Cir. 2010) 631 F.3d 266, 285.

[11] **NOTE**: The lack of cases occurred because, as discussed below, the exclusionary rule does not apply to SCA violations; thus, there are no cases in which criminal defendants sought the suppression of evidence.

When the SCA applies

Theoretically, the first step in determining how to obtain copies of electronic communications is to figure out whether the communication falls within the protections of the SCA. In reality, however, it doesn't really matter because, even if the law does not apply (or even if the message was not "private" under the Fourth Amendment), officers will seldom be able to obtain any stored communication from a service provider unless they have legal authority for doing so. This is because providers risk being sued by their subscribers if they reveal communications without legal process. So they usually insist upon it.

In any event, a message falls within the SCA if (1) it was "stored," and (2) it was stored on the equipment of an "electronic communication service" (ECS) or a "remote computing service" (RCS).

WHAT'S A "STORED" COMMUNICATION? An electronic communication is deemed "stored" if it was being held temporarily by a provider as an incident to its transmission to the recipient. Thus, most courts have ruled that an email or other communication that has been opened by the recipient is no longer in temporary storage because it has reached its final destination.[12]

It should be noted, however, that the Ninth Circuit muddied things up when it announced its controversial decision in the case of *Theofel* v. *Farley-Jones.*[13] In *Theofel*, the court broadly defined the term "storage" to include the storage of all email held by a provider until it is "expired in the normal course" (whatever that means), even if it has been opened and is therefore no longer being stored incident to or pending delivery. Among the critics of this ruling was the preeminent authority on the subject who observed that "the Ninth Circuit's analysis in *Theofel* is quite implausible and hard to square with the statutory text."[14] In addition, the U.S. Department of Justice has written that "the Ninth Circuit's reasoning in *Theofel* confuses 'backup protection' with ordinary storage of a file."[15] But, for now, *Theofel* is still the law in this circuit.

ECSS AND RCSS: The SCA regulates the disclosure of electronic communications that are in the possession of an ECS or RCS available to the general public. Here, the term "electronic communication service" is broadly defined as "any service which provides to users thereof the ability to send wire or electronic communications,"[16] which would include internet, telephone, and email service providers.[17] In contrast, a website such as Amazon.com would not be deemed an ECS because it is in the business of processing sales orders which are not the type of communication that is covered under the SCA.[18]

As for "remote computing services," they are companies that provide "computer storage or pro-

[12] See *Steve Jackson Games, Inc.* v. *U.S. Secret Service* (5th Cir. 1994) 36 F.3d 457, 461; *DoubleClick Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 511-12; *Fraser* v. *Nationwide Mutual Insurance Co.* (E.D. Pa. 2001) 135 F.Supp.2d 623, 635-36.

[13] (9th Cir. 2003) 359 F.3d 1066.

[14] Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1217. Also see *U.S.* v. *Weaver* (C.D. Ill. 2009) 636 F.Supp.2d 769, 772 ["The Ninth Circuit's interpretation of storage for backup protection under the Stored Communication Act cannot be squared with legislative history and other provisions of the Act."].

[15] Computer Crime and Intellectual Property Section [of DOJ], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Chapter 3 The Stored Communications Act), www.cybercrime, gov/ssmanual/03ssma.html, accessed September 2011.

[16] 18 U.S.C. § 2510(15).

[17] See *Quon* v. *Arch Wireless* (9th Cir. 2008) 529 F.3d 892, 903 [text messaging service was deemed an ECS] [overturned on other grounds in *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]; *In re DoubleClick Inc. Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 508 ["Access to the Internet is the service an ISP provides. Therefore, the 'service which provides to users thereof the ability to send or receive wire or electronic communications' is 'Internet access.'"]; *Freedman* v. *America Online* (E.D. Va. 2004) 325 F.Supp.2d 638, 643, fn.4 ["It is clear that AOL is a provider of 'electronic communication service'"].

[18] See *Crowley* v. *CyberSource Corp.* (N.D. Cal. 2001) 166 F.Supp.2d 1263, 1270 ["Crowley argues that Amazon is an electronic communication service provider because it receives electronic communications from customers, saying that 'without recipients such as Amazon.com, users would have no ability to send electronic information.' This argument was expressly rejected in *Andersen Consulting LLP* v. *UOP*, 991 F.Supp. 1041 (N.D.Ill.1998)."]; *In re Jetblue Airways Corp. Privacy Litigation* (E.D.N.Y. 2005) 379 F.Supp.2d 299, 307 ["Thus, a company such as JetBlue does not become an "electronic communication service" provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers."]; *Dyer* v. *Northwest Airlines Corp.* (D.N.D. 2004) 334 F.Supp.2d 1196, 1199 ["Courts have concluded that 'electronic communication service' encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online."].

cessing services by means of an electronic communications system."[19] Thus, while most ECSs simply transmit and temporarily store information as an incident to the communication, RCSs store the information for other purposes, and may process it or otherwise make changes to it.[20]

It should be noted that the distinction between ECSs and RCSs is a holdover from 1980s technology and is no longer of much importance. That is because most people now utilize the services of internet service providers who are almost always ECSs or, at least, multifunctional.[21]

SEARCHING THE SUSPECT'S COMPUTER: It is important to understand that the procedures set forth in the SCA do not cover searches of email, voicemail, or text messages that have been stored on computers or other storage devices that are owned or controlled by the suspect. There are two reasons for this. First, the SCA covers only communications that have been stored with third-party providers. Second, even under *Theofel,* messages stored on a suspect's computer are not in temporary or intermediate storage because they do not "expire in the normal course."[22] But even though the SCA does not apply, the Fourth Amendment *does*, which means that officers will need a warrant to search a suspect's computer.

Communications vs. Records

Although the federal law is known as the Stored Communications Act, it also provides the means by which officers can obtain the *records* pertaining to those communications. This is significant because communication records often provide information that is just as important as the communications themselves. For example, investigators may be able to determine a suspect's whereabouts at a particular time by obtaining records that reveal the locations of cell phone towers that carried signals from his phone.

The SCA's role in obtaining records is also important because, while a search warrant is usually necessary to obtain communications, there are several other options when officers are seeking records. Because of this, and because communication records are so important to investigators, this subject is covered in a separate article starting on page 8.

The difference between communications and communications records is not, however, as clear cut as it might seem—especially when dealing with electronic communications. For this reason, it is necessary to briefly discuss these differences.

The term "electronic communications" (also called "content") refers to the message that is conveyed by the sender, including statements of fact, thoughts, requests, conclusions and other expressions. Thus, the federal wiretap law defines the term "contents" as including "any information concerning the substance, purport, or meaning of that communication."[23] Importantly, words may be deemed "communications" even if they are not technically a part of the message. For example, the subject line pertaining to an email message would likely be deemed "content."[24]

---

[19] 18 U.S.C. § 2711(2).

[20] **NOTES**: According to the U.S. Department of Justice, "Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer," such as a "service provider that allows customers to use its computing facilities" or a "server that allows users to store data for future retrieval." Computer Crime and Intellectual Property Section [of DOJ], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Chapter 3 The Stored Communications Act), www.cybercrime, gov/ssmanual/03ssma.html, accessed September 2011.

[21] **NOTE**: For these reasons, a respected commentator in this area of the law has recommended that Congress eliminate "the confusing" ECS and RCS categories. Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1209, 1215.

[22] See 18 U.S.C. 2510(17) ["electronic storage" means (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication *by an electronic communication service* for purposes of backup protection of such communication"; emphasis added].

[23] 18 U.S.C. § 2510(8). Also see 18 U.S.C. 2711(1); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act*, 97 Nw U.L.Rev. 607, 611 ["[E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communication."].

[24] See *In re Application of the U.S.* (D. Mass 2005) 396 F.Supp.2d 45, 48 ["the information contained in the 'subject' would reveal the contents of the communication"]; Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1228 ["the subject line generally carries a substantive message"].

In contrast, "records" consist of raw data that is merely ancillary to the communication.[25] Examples include the "to/from" names and addresses, dates, and times pertaining to an email message, the phone numbers that were transmitted to telephone switching equipment, the addresses of websites that were visited on a certain computer, and the internet or IP address assigned to a particular computer.[26] While it is true that such raw data might permit officers to draw some conclusions as to a person's interests or other private matters, it will ordinarily be deemed a "record"—not a "communication." As the Ninth Circuit explained in *U.S.* v. *Forrester*:

> When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a prerecorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the [Supreme Court has drawn] a clear line between unprotected addressing information and protected content information . . .[27]

It should be noted, however, that while the locations of websites a person visited are considered records, it is possible, that Uniform Resource Locators (URLs) will be deemed content because they indicate "the location of specific documents on the Web" that a person has viewed and, thus, constitute the type of "personal information" that may be entitled to greater protection.[28]

How to Obtain Communications

Now we get to the heart of the matter: How can officers obtain copies of email, voicemail, and text messages from providers? As we will discuss, there are five ways, but only one of them—a search warrant—has much practical importance in California.

SEARCH WARRANTS: In most cases, officers should seek a search warrant if they have probable cause to believe that certain email, voicemail, or text messages constitute evidence of a crime. There are four reasons for this:

(1) REQUIRED FOR NEW MESSAGES: The SCA requires a warrant if, as is usually the case, officers want to search for messages that have been in storage for 180 days or less.[29]

(2) AUTHORIZED BY CALIFORNIA LAW: The California Penal Code expressly authorizes the issuance of search warrants for this purpose.[30]

(3) PROVIDER MAY REQUIRE IT: Although the SCA permits the release of communications by means of a subpoena or a D-Order (discussed below), some providers insist upon search warrants so as to eliminate any possibility of liability resulting from disclosure.

(4) THE JUDGE MAY REQUIRE IT: Because the law in this area is somewhat inarticulate (especially the sufficiently of D-Orders), some judges have refused to authorize the release of electronic communications by any means other than a search warrant.

---

[25] See *Smith* v. *Maryland* (1979) 442 U.S. 735. 741 ["Yet a pen register differs significantly from [a listening device] for pen registers do not acquire the *contents* of communications."].

[26] See *In re § 2703(d) Order* (E.D. Va. 2011) 787 F.Supp.2d 430, 436 ["The Twitter Order does not demand the contents of any communication, and thus constitutes only a request for records"].

[27] (9th Cir. 2008) 512 F.3d 500, 510.

[28] See *In re Pharmatrak Privacy Litigation* (1st Cir. 2003) 329 F.3d 9, 13, 16.

[29] See 18 U.S.C. § 2703(a); *U.S.* v. *Warshak* (6th Cir. 2011) 631 F.3d 266, 283 ["The government may obtain the contents of e-mails that are in electronic storage with an electronic communications service for 180 days or less only pursuant to a warrant."].

[30] Pen. Code § 1524.2.

Furthermore, in a decision that has drawn a lot of discussion, the Sixth Circuit ruled in *United States.* v. *Warshak*[31] that, while the Stored Communications Act permits the acquisition of email by means of a D-Order, the Fourth Amendment does not. The court reasoned that people who communicate via email can and do reasonably expect that their communications will remain private. And this means that the release of these communications to law enforcement is governed by the Fourth Amendment (in addition to the SCA). Consequently, as in most intrusions that are deemed "searches," a warrant will be required unless there is an exception to the warrant requirement, such as emergency or consent. Said the court:

> It only stands to reason that, if government agents compel an [internet service provider] to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.[32]

Commenting on this ruling, CNET.com said, "The decision, assuming it survives a potential appeal to the U.S. Supreme Court, marks a major turning point in the evolution of Fourth Amendment law in the Digital Age."[33]

Two other things should be noted about *Warshak*. First, the Ninth Circuit has indicated it agrees with the court's analysis.[34] Second, while decisions of the federal circuits courts are not binding on California courts, a well-reasoned case such as *Warshak* may have substantial persuasive value.[35]

There are some other things about search warrants that should be noted:

NO NOTICE TO SUBSCRIBER: Officers are not required to notify the subscriber that a warrant for his communications or records was executed.[36]

NOTICE TO PRESERVE: Because providers routinely delete email and other stored electronic communications, and also because subscribers may be able to delete their own messages, the SCA provides that ISPs must preserve these messages for 90 days if officers request them to do so.[37] Accordingly, when officers determine that voicemail, email, or text messages may be relevant to an investigation, they should immediately contact the provider, give notice that a warrant will be sought, and request that they save any stored messages.

PRESERVATION REQUIRED: A provider who receives a preservation request must "take all necessary steps to preserve records and other evidence in its possession," and must retain it for 90 days.[38] A 90-day extension must be granted if officers request it.

NONDISCLOSURE ORDERS: If an investigation would be jeopardized if the suspect knew that officers had obtained copies of his email, voicemail, or text messages, officers may seek a nondisclosure order prohibiting the service provider from releasing this information to the customer for 90 days.[39] Grounds for a such an order will exist if officers reasonably believed that disclosure would (1) endanger the life or safety of a person, (2) result in flight from prosecution, (3) result in destruction of or tampering with evidence, (4) result in the intimidation of a potential witness, or (5) would otherwise seriously jeopardize the investigation or unduly delay a trial.[40] A court may order 90-day extensions of a nondisclosure order.[41]

---

[31] (6th Cir. 2010) 631 F.3d 266, 286.
[32] But also see *Rehberg* v. *Paulk* (11th Cir. 2010) 611 F.3d 828, 847 ["No Supreme Court decision and no precedential decision of this Circuit defines privacy rights in email content voluntarily transmitted over the global Internet and stores at a third-party ISP."].
[33] Larry Downes, "Search warrants and online data: Getting real," CNET News (December 15, 2010).
[34] See *U.S.* v. *Forrester* (9th Cir. 2008) 512 F.3d 500, 511 ["The privacy interests in these two forms of communication [i.e., email and physical mail] are identical."].
[35] See *People* v. *Bradford* (1997) 15 Cal.4th 1229, 1305 ["Such decisions, as we often have observed, provide persuasive rather than binding authority."].
[36] See Pen. Code § 1524.3(b) ["A governmental entity receiving subscriber records or information [by means of a search warrant] is not required to provide notice to a subscriber or customer."].
[37] See 18 U.S.C. § 2703(f).
[38] See Pen. Code § 1524.3(d); 18 USC § 2703(f).
[39] See 18 U.S.C. §2705(a)(1).
[40] See 18 USC § 2705(a)(2).
[41] See 18 U.S.C. 2705(a)(4)

WARRANTS ON OUT-OF-STATE ISPS: A judge in California may issue a search warrant for records stored in another state if the provider is doing business here.[42]

SERVING CORPORATIONS: A warrant for stored communications in the possession of a California corporation and most out-of-state corporations may be served by means of U.S. mail, overnight delivery service, fax, or hand delivery to (1) any officer or general manager located in California, or (2) its agent for service of process.[43] It is also a good idea to send a copy of the warrant to the provider's law enforcement liaison, if any. Note that the Penal Code requires that foreign corporations produce the requested communications within five business days of receipt, although the judge may require the production of such communications in less than five days if investigators establish good cause, such as a danger to life or flight from prosecution.[44]

REIMBURSEMENT: A law enforcement agency that obtains email, voicemail, or text messages from a service provider by means of a search warrant or otherwise must reimburse the company "for such costs as are reasonably necessary, and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information."[45]

D-ORDERS: The SCA states that officers may, under certain circumstances, obtain copies of email, voicemail, and text messages by means of a court order, commonly known as a "2703(d) Order" or simply a "D-Order." The advantage of a D-Order is that it does not require probable cause. Instead, a court may issue such an order if the accompanying application contains "specific and articulable facts" that establish "reasonable grounds" to believe that the contents of the communication "are relevant and material to an ongoing criminal investigation."[46] One disadvantage of D-Orders is that officers must ordinarily give the subscriber notice that they will be seeking one so that he may obtain judicial review.[47]

D-Orders are, however, controversial because they permit the release of private communications on less than probable cause. Thus, judges may not issue them. Furthermore, when we went to press the U.S. Senate was considering a bill that would generally prohibit the release of such communications except by means of a search warrant.

SUBPOENA: Although the SCA also permits the release of electronic communications by means of subpoena, the subpoena procedure in California is so restrictive that, as a practical matter, subpoenas are seldom useful.[48]

CONSENT: An ISP may release copies of an email, voicemail, or text message to officers if the sender or recipient consented to the release in writing.[49]

EMERGENCIES: The SCA permits providers to voluntarily disclose stored communications to law enforcement officers if (1) the provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay," (2) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto" under 42 U.S.C. §13032, or (3) the provider learned of the communication "inadvertently" and determined that it pertained "to the commission of a crime."[50] POV

---

[42] See Pen. Code § 1524.2; Code Civ. Proc. § 410.10; Corp. Code § 2105(a)(5); *People* v. *Stipo* (2011) 195 Cal.App.4th 664, 671.
[43] See Pen. Code § 1524.2(a)(6); Corporations Code § 2110; 18 USC § 2703(g).
[44] See Pen. Code § 1524.2.
[45] See 18 U.S.C. § 2706.
[46] 18 U.S.C. § 2703(d).
[47] See 18 USC § 2703(b)(1)(B)(ii).
[48] See Pen. Code §§ 1326, 1327; Evid. Code § 1560; *People* v. *Superior Court (Barrett)* (2000) 80 Cal.App.4th 1305, 1315 [a subpoena duces tecum requires the person served "to produce information in court"]; *Carlson* v. *Superior Court* (1976) 58 Cal.App.3d 13, 22 ["[L]aw enforcement officials may not gain access to an accused's private papers by subpoena until there has been a judicial determination there is probable cause to believe he has committed a criminal offense and that the papers [are evidence]."].
[49] See 18 U.S.C. § 2702(b)(3); *S.E.C.* v. *Jerry T. O'Brien, Inc.* (1984) 467 U.S. 735, 743 [an ISP may divulge the contents of an email "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"].
[50] See 18 U.S.C. § 2702(c).