# Phone, E-mail, and Internet Records

*"Investigators in the Michael Jackson child molestation case have seized about 100 pages of phone records at his Neverland Ranch according to court documents."*
*Los Angeles Daily News*, March 2, 2004.

Sometimes the most incriminating evidence in a criminal investigation is a scrap of raw data. A name or address. A phone number. A credit card number. Things like that. This type of information is also a well-known source of leads to important witnesses and physical evidence.

There are several sources for this type of information, but the most accessible and reliable is often a company that provides phone, e-mail, or internet service. After all, most people in the United States—especially those who live in California—have an account with one or more these companies.[1]

Basic account records are not, however, the only type of information these companies can provide. In fact, their computers are constantly collecting and storing all sorts of data that may be important in a case. Among other things, phone and e-mail companies may know who a suspect or victim has been communicating with and precisely when those communications took place. Internet service providers keep tabs on what web sites people have visited and when they were logged on.

Of growing interest to investigators is the ability of cell phone companies to track the whereabouts of a suspect at a particular time by checking the location of cell phone antenna towers that were in contact with his cell phone. For example, ABC News reported last July that "cell phone records of the man accused in the abduction, sexual abuse and murder of 5-year-old Samantha Runnion reportedly put the suspect in the area where the girl's body was found."

In discussing the importance of phone records in many criminal investigations, the California Supreme Court made this observation in 1979:

> It is virtually impossible for an individual or business entity to function in the modern economy without a telephone, and a record of telephone calls provides a virtual current biography.[2]

That's still true today—but now a person's "virtual current biography" might also be found in the records of companies that provide e-mail and internet service.[3]

The question, then, is what must officers and prosecutors do to obtain this information? The question is fairly straightforward, yet this is an area of the law that causes some uncertainty. There are essentially two reasons for this. First, it is regulated by both federal and state law. Thus, investigators must understand and comply with two sets of laws which, as often happens, are not clearly written and are subject to differing interpretations.

---

[1] NOTE: "Millions of people now have electronic mail addresses. Businesses, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line. Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place." House Report No. 103-827 on the Communications Assistance for Law Enforcement Act at p. 17. ALSO SEE *Freedman* v. *AOL* (E.D. Va 2004) __ F.Supp.2nd __ ["AOL typically responds to approximately 1000 [search] warrants per month from authorities all over the country."].

[2] *People* v. *Blair* (1979) 25 Cal.3d 640, 653.

[3] NOTE: Internet service providers will soon be going into the telephone business, furnishing subscribers with the ability to have phone conversations over the internet via so-called Voice-Over Internet Protocol (VOIP) technology.

Second, officers cannot ordinarily obtain this information without the help of the provider; e.g., a phone company. And although most providers willingly cooperate with officers, some demand legal process beyond what is required by the law. They do this, or so they say, because they worry about being sued by their customers for complying with court orders and search warrants. But because these providers are virtually immune from liability for complying with court orders, this explanation is dubious.[4] In any event, it sometimes happens that officers and prosecutors who have done everything they are required to do by the law will be told by the provider that it's not enough. This can result in delays that seriously impair the investigation.

For example, Hayward homicide investigators obtained a search warrant last year for AT&T Wireless voicemail messages left for a murder victim shortly before he was killed. They needed this information because there were few clues in the case and they thought it would help if they knew the identities of the people who recently spoke with the victim and what, if any, messages they left. But AT&T Wireless refused to turn over the tapes unless the officers obtained a *wiretap* order. This was, of course, preposterous, and a judge so ruled. But the delay seriously delayed the investigation. (We were informed by Glendale police investigators that they recently had the same problem with AT&T Wireless.)

One final note. We have prepared several forms that officers and prosecutors may use to obtain records from telephone, e-mail, and internet providers. Those forms are as follows:

- Court order and application for telephone, e-mail, and internet records
- Search warrant for same
- Emergency declaration for same
- Court order for phone pen register/trap-trace
- Court order for e-mail pen register/trap-trace

These forms may be viewed on the Alameda County DA's Office website at www.acgov.org/da. Click on "Forms for officers." To obtain these forms in Microsoft Word format, e-mail a request to alcoda@acgov.org and we will e-mail them to you.

## AN OVERVIEW

To understand this area of the law, it will be helpful to start with the basics. First off, all electronic communications data are classified as "stored records," as opposed to intercepted content.

"RECORDS" VS. "CONTENT": There are two types of information that can be obtained from electronic communications services: records and content. "Content" is the actual communication, typically the words spoken by the parties to a telephone conversation or the message contained in an e-mail.[5] "Records," on the other hand, consist of raw data pertaining to a communication.[6]

---

[4] See 18 USC § 2707(d); Penal Code § 1524.3(e).

[5] See 18 USC § 2510(8) ["Contents" defined: "(W)hen used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"]. ALSO SEE *Jessup-Morgan* v. *AOL* (1998) 20 F. Supp.2d 1105, 1108 ["The 'content' of a communication is not at issue in this case. Disclosure of information identifying an AOL electronic communication account customer is at issue."]; *In re application of the USA for an order authorizing the use of a cellular telephone digital analyzer* (1995) 885 F.Supp. 197, 199 [a cell phone's ESN, its own number, and the numbers being called by the cellular telephone are not "content"].

[6] See *Smith* v. *Maryland* (1979) 442 US 735, 741 ["Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."]. ALSO SEE *Merriam-Webster's Collegiate Dictionary* (11th ed. 2003) p. 1040:

For example, in an e-mail the names of the sender and recipient, their e-mail addresses, and the date and time the message was sent and opened are all records. But the message and the subject line are "content" because they are intended to communicate thoughts. Similarly, the telephone numbers transmitted to a pager are "records." But a numeric message transmitted to the same pager is "content."[7]

"STORAGE" VS. "INTERCEPTION": In addition to classifying information by its nature (content vs. records), the law categorizes it as either "stored" or "intercepted." Information is "intercepted" if officers obtained it while it was in-transit.[8] For example, wiretaps and audio bugs record conversations as they are happening and, therefore, they "intercept" them.

In contrast, "stored" records are obtained after they have been saved—on paper, tape, or digitally—for future retrieval or transmission.[9] For example, phone company records that list the phone numbers dialed by a customer are saved—"stored"— by the company for billing purposes.

WHY THESE CLASSIFICATIONS ARE IMPORTANT: The significance of these classifications is that "stored records" are not deemed private under the Fourth Amendment.[10] This is because, (1) subscribers know that their communications records

---

Record: "(A) body of known or recorded facts about something or someone esp. with reference to a particular sphere of activity . . . ."; Dictionary.com: Data: "(1) Factual information, especially information organized for analysis or used to reason or make decisions. (2) *Computer Science.* Numerical or other information represented in a form suitable for processing by computer."

[7] See *Brown* v. *Waddell* (4th Cir. 1995) 50 F.3d 285, 287-8 ["Waddell intercepted a number of numeric messages containing more extensive sets of numbers than those in telephone numbers, including at least one that was conceded to be a code indicating that a caller which it identified as 'en route.'"]; *People* v. *Pons* (1986) 509 N.Y.S. 2d 450, 453 ["The monitoring of [a] telephone pager device is more intrusive than the use of a pen register. The pager device is capable of conveying substantive information by combining digits in various sequences. Both telephone numbers and coded messages may be conveyed."].

[8] See *Fraser* v. *Nationwide Mut. Ins. Co.* (3rd Cir. 2003) 252 F.3d 107, 113 ["(W)e agree with Nationwide. Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."].

[9] See 18 USC § 2701 et seq. ALSO SEE *In re Pharmatrak* (1st Cir. 2003) 329 F.3d 9, 21-2 ["Traveling the internet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox." Quoting from *U.S.* v. *Councilman* (D.Mass. 2003) 245 F.Supp.2d 319, 321; *State* v. *Townsend* (2002) 57 P.3d 255, 260 ["A person sends an e-mail message with the expectation that it will be read and perhaps printed by another person. To be available for reading or printing, the message first must be recorded on another computer's memory. Like a person who leaves a message on a telephone answering machine, a person who sends an e-mail message anticipates that it will be recorded. That person thus implicitly consents to having the message recorded on the addressee's computer."]; *Quon* v. *Arch Wireless Operating Co.* (2004) 2004 WL 581355 ["The [Stored Communications Act] relates to electronic messages that are not intercepted, but rather are extracted from electronic storage."].

[10] See *Smith* v. *Maryland* (1979) 442 US 735, 743-4 ["This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."]; *U.S.* v. *Konop* (9th Cir. 2002) 302 F.3d 868, 879 ["The level of protection provided stored communications under the [Stored Communications Act] is considerably less than that provided communications covered by the Wiretap Act. Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act."]; *Guest* v. *Leis* (6th Cir. 2001) 255 F.3d 325, 335-6 ["Individuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties. . . . Courts have applied this principle to computer searches and seizures to conclude that computer users do not have a legitimate expectation of

are saved and can, therefore, be viewed by company employees and given to law enforcement officers under certain circumstances, and (2) when the subscriber sent the record, he knowingly surrendered all control over it to the provider.

For example, when a person dials a phone number, that number is automatically stored on equipment owned by his phone company. Thus, in *Smith* v. *Maryland*, the U.S. Supreme Court ruled the defendant did not have a reasonable expectation of privacy as to the numbers he dialed on his phone because, said the Court:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In doing so, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[11]

ELECTRONIC COMMUNICATIONS PRIVACY ACT: Although electronic communications records are not private under the Fourth Amendment, Congress has determined that people who communicate via telephone, e-mail, and the internet have a sufficient privacy interest in the records of their communications to warrant at least some legal restrictions on their release to law enforcement. Consequently, in 1986 it enacted the Electronic Communications Privacy Act (ECPA) which, among other things, sets forth the procedure by which federal and state officers can obtain this information.[12] This procedure will be covered later in this article.

"ELECTRONIC COMMUNICATION SERVICE": The procedures set forth in the ECPA for obtaining communications records are not limited to data in the hands of phone companies. In fact, the ECPA was enacted in 1986 because the law needed to adapt to the new ways in which people were communicating.[13] As the result, the ECPA applies to companies that provide an "electronic communication service" which is defined very broadly to include any company that "provides to users thereof the ability to send or

---

privacy in their subscriber information because they have conveyed it to another person—the system operator."]; *People* v. *Lissauer* (1985) 169 Cal.App.3d 413, 419 [no reasonable expectation of privacy as to telephone company's records containing the subscriber's name and address]; *U.S.* v. *Meriwether* (6th Cir. 1990) 917 F.2d 955, 959 [no reasonable expectation of privacy in phone number sent to pager]; *U.S.* v. *Meek* (9th Cir. 2004) 366 F.3d 705, 711 ["Like private telephone conversations, either party to a chat room exchange has the power to surrender each other's privacy interest to a third party. The nature of consent illustrates a reality of the Internet, namely, that a person initiating an Internet-based conversation does not control the recipient."]; *People* v. *Medina* (1987) 189 Cal.App.3d 39, 43-5 [no reasonable expectation of privacy when defendant sent and received verbal messages over a pager in which all messages were transmitted over a single frequency and could be overheard by other subscribers to the paging service]; *In re Application of the USA for an order authorizing the installation and use of a pen register and trap and trace device* (1994) 846 F.Supp. 1555, 1558 ["*Smith* v. *Maryland*) compels the conclusion that (absent some presently unforeseen, aggravating circumstance) no constitutionally cognizable issues inhere in law enforcement's resort to a pen register."].

[11] (1979) 442 US 735, 744.

[12] See *In re application of the USA* (2001) 157 F.Supp.2d 286, 288 ["The ECPA provides a statutory mechanism under which the Government can obtain a court order directing a company that provides 'electronic communication service' to disclose certain subscriber records . . . "]; *U.S.* v. *Councilman* (1st Cir. 2004) __ F.3d __ ["The Electronic Communications Privacy Act ('ECPA') amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, commonly known as the federal wiretap law. The ECPA was divided into Title I, commonly known as the Wiretap Act, and Title II, commonly known as the Stored Communications Act."].

[13] See *In re Application of the USA for an Order Pursuant to 18 USC § 2703(d)* (2001) 157 F.Supp.2d 286, 289 ["Title III was amended in 1986 because of the belief that it had not kept pace with the development of communications and computer technology."].

receive wire or electronic communications."[14] As the U.S. District Court in New York observed, this definition encompasses a variety of businesses:

> The ECPA was intended to apply to large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing. Thus, it has been repeatedly recognized that the ECPA applies to electronic communications transmitted via the internet.[15]

ECPA VIOLATIONS: Because the Fourth Amendment does not view communications records as private, records cannot be suppressed on grounds they were obtained in violation of the ECPA.[16] Officers who violate the ECPA may, however, be sued.[17]

COMPENSATION TO PROVIDERS: A law enforcement agency that obtains communications records by means of a court order or search warrant must compensate the provider for its reasonable expenses in furnishing the records (other than telephone toll records and telephone listings).[18]

HOW TO OBTAIN RECORDS: As discussed later, there are essentially four ways in which investigators can obtain communications records: (1) court order, (2) search warrant, (3) subpoena,[19] and (4) emergency declaration.

STATE SEARCH WARRANTS AND COURT ORDERS: Although the ECPA is a federal law, it specifically authorizes state judges, under certain circumstances, to order the release of communications records by means of state search warrants and court orders.[20]

---

[14] See 18 USC §2510(15); *Quon* v. *Arch Wireless* (2004) __ F.Supp.2d __ ["An 'electronic communication service' is defined as 'any service which provides to users thereof the ability to send or receive wire or electronic communications.' A 'user' is defined as 'any person or entity who (A) uses an electronic communication service; and (B) is duly authorized.'"].

[15] See *In re Application of the USA for an Order Pursuant to 18 USC § 2703(d)* (2001) 157 F.Supp.2d 286, 289.

[16] See *People* v. *Larkin* (1987) 194 Cal.App.3d 650, 653 ["Because warrantless uses of a pen register do not violate the Fourth Amendment, the exclusionary rule is not applicable."]; *U.S.* v. *Thompson* (11th Cir. 1991) 936 F.2d 1249, 1252 ["When Congress specifically designates a remedy for one of its acts, courts generally presume that is engaged in the necessary balancing of interests in determining what the appropriate penalty should be. Absent a specific reference to an exclusionary rule, it is not appropriate for the courts to read such a provision into the act."]; *U.S.* v. *Kennedy* (2000) 81 F.Supp.2d 1103, 1110 ["Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA. The statute specifically states that 'the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."]; *U.S.* v. *Smith* (9th Cir. 1998) 155 F.3d 1051, 1056.

[17] See 18 USC § 2707; *Tucker* v. *Waddell* (4th Cir. 1996) 83 F.3d 688, 691 ["(The ECPA) authorizes a private cause of action against governmental entities that violate the Electronic Communications Privacy Act."].

[18] See 18 USC § 2706 [subscriber and transaction records]; 18 USC § 3124(c) [pen register and trap-trace].

[19] NOTE: We will not discuss subpoenas because they are seldom used to obtain communications records in the course of a criminal investigation. The authority for release of records by means of subpoena is 18 USC § 2703.

[20] See 18 U.S.C. §§ 2703(d) [telephone records] 3122(a)(2) [pen registers and phone traps]; Penal Code § 1524.2; *Brown* v. *Waddell* (4th Cir. 1995) 50 F.3d 285, 290 ["(U)nless prohibited by state law, state law enforcement officers (not just principal prosecutors) may obtain authorization for use of these devices from state courts"]. NOTE: The California Attorney General's Office (AG) has opined that California law prohibits the use of a court order to obtain pen register and phone trap data (opinion 03-406). But, as we explained in the Spring 2004 edition of *Point of View*, its conclusion in untenable. It should also be noted that when the DA's of Alameda and Los Angeles counties provided the AG with separate points and authorities demonstrating why its conclusion

GEOGRAPHICAL SCOPE OF SEARCH WARRANTS AND COURT ORDERS: Search warrants and court orders issued by federal judges are binding on all electronic communication services in the U.S.[21] Warrants and orders issued by judges of the Superior Court of California are binding on all providers that are, (1) headquartered in California, or (2) doing business in California.[22]

PRESERVATION OF RECORDS: Some communications records are erased or otherwise destroyed as a matter of course. To help prevent the destruction of relevant records, officers should immediately notify the company when they realize the records may be needed in their investigation. Under federal law, when such a request is made the provider must "take all steps to preserve records and other evidence in its possession" for 90 days, pending issuance of a court order or search warrant.[23] The statute also provides for a 90-day extension.

WHAT RECORDS ARE AVAILABLE: The records that can be obtained from electronics communication services fall into three categories: (1) basic subscriber information, (2) transactional records, and (3) records obtained by means of pen registers and connection traps.

## BASIC SUBSCRIBER AND TRANSACTION RECORDS

There is no significant difference between the procedures for obtaining basic subscriber information and those for obtaining transaction records. Consequently, these subjects are discussed together.[24]

### Available information

The following information is ordinarily available to investigators.

BASIC SUBSCRIBER INFORMATION: This includes the subscriber's name, address, phone number, length of service with the provider, the types of services utilized (e.g. call forwarding), and the means and source of payment (including credit card and bank account numbers).[25]

---

was wrong, the AG failed to refute them. Instead, it responded lamely that it was standing by its opinion. The AG's failure to respond to thoughtful legal arguments from two DA's offices speaks volumes as to the worth of this ill-advised opinion. While thoughtful reasoning in an AG's opinion may have some convincing force, the strained and feeble analysis in this opinion betrays its unsoundness.

[21] See 18 USC §§ 2703(d), 2711(3), 3123(a), 3127.

[22] See Code of Civil Procedure § 410.10 ["A court of this state may exercise jurisdiction on any basis not inconsistent with the Constitution of this state or of the United States."]; *Burger King Corp.* v. *Rudzewicz* (1985) 471 US 462, 476 [when the out-of-state defendant "manifestly has availed himself of the privilege of conducting business [in the forum state], and because his activities are shielded by the benefits and protections of the forum's laws it is presumptively not unreasonable to require him to submit to the burdens of litigation in that forum as well."]. NOTE: When serving the warrant in such a manner, consider including a copy of Penal Code § 1524.2(a)(6) so that the provider will know that it has been legally served.

[23] See 18 USC § 2703(f). ALSO SEE Penal Code § 1524.3 (d) [upon the request of a peace officer, the provider "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a search warrant. . . . Records shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon renewed request by the peace officer."].

[24] NOTE: To determine the name of the telephone company that provides service to a particular phone, officers can go to www.fonefinder.net.

[25] See 18 USC § 2703(c)(2).

An example of the types of internet information that is available is found in the case of *United States* v. *Kennedy*.[26] In *Kennedy*, FBI agents obtained the Internet Protocol (IP) address of a computer on which child pornography had been downloaded. With this number and the name of the suspect's internet service provider (ISP), they obtained a court order requiring the ISP to furnish all subscriber information on that account. As the result, the FBI received the following information:

> The subscriber whose computer used I.P. address 24.94.200.54 on July 2, 1999, at 11:49 P.M. was Rosemary D. Kennedy of 9120 Harvest Court, Wichita, Kansas, telephone 316-722-6593. Two users were listed for that account: rkennedy@kscable.com and kennedy@kscable.com. The account had been active since June 7, 1999.

TRANSACTION RECORDS: Transaction records contain information about the subscriber's use of a telephone, e-mail, or internet service.[27] These include the following:

> TELEPHONE CONNECTION RECORDS: Local and long distance telephone connection or billing records, such as the date and time each call was made or received, and the length of each call. (This information is especially useful when officers need to learn the identities of the suspect's associates or establish a connection between a suspect and others, such as co-conspirators.)
>
> LAST CALL RECORDS: The last number dialed on the target phone, and the number of the phone from which the last call to the target phone was placed.[28]
>
> CELL TOWER HITS: Records showing the locations of cell phone antenna towers that had been in contact with the target cell phone and the time when each contact was made.
>
> DIGITAL ANALYZER DATA: This is a portable device which, when near a cell phone, detects its phone number, ESN, and numbers dialed.[29] It is unsettled whether court authorization is required. But if so, an order analogous to one that authorizes a pen register/connection trap operation ought to suffice.[30]

---

[26] (2000) 81 F.Supp.2d 1103.

[27] See 18 USC § 2703(c)(2)(C); *Hill* v. *MCI* (2000) 120 F.Supp.2d 1194, 1195 [transaction information included "invoice/billing information and the names, addresses, and phone numbers of parties [the defendant] called"]; *U.S.* v. *Allen* (2000) 53 MJ 402, 409 ["The information obtained from 'Super Zippo' was electronic data stored by 'Super Zippo' in the form of a log identifying the date, time, user, and detailed internet address of sites accessed by appellant over several months. Hence, it falls within [18 USC 2703(c)]."]; House Report No. 103-827 (1994) [Communications Assistance for Law Enforcement Act] pp. 10, 17, 31.

[28] NOTE: Do not delay: This information may be lost when a new number is dialed from the phone or when someone places a call to the phone. This may happen even if the phone is unplugged or taken off the hook. Consequently, officers should immediately notify the phone company as soon as they determine they will need this information. The phone company will then hold the number pending receipt of a court order, search warrant, or emergency declaration.

[29] See *In re application of the USA for an order authorizing the use of a cellular telephone digital analyzer* (1995) 885 F.Supp. 197, 198-9 ["A cellular telephone digital analyzer is a portable device that can detect signals emitted by a cellular telephone. The digital analyzer can detect the electronic serial number (ESN) assigned to a particular cellular telephone, the telephone number of the cellular telephone itself, and the telephone numbers called by the cellular telephone."].

[30] See *In re Cellular Telephone Digital Analyzer* (C.D. California 1995) 885 F.Supp. 197. 201. NOTE: If the number of the cell phone to be analyzed is not known at the time the order is sought, officers will be unable to comply with the requirement that the court order specify the number. See 18 USC 3123(b)(1)(C). In any event, this requirement may be satisfied if, (1) officers maintain "a time log identifying each target cellular telephone analyzed (by ESN and telephone number), together with all intercepted telephone numbers dialed or pulsed from each telephone. Id. at p. 202.

E-MAIL, CHAT SESSION RECORDS: Records of e-mail and internet session times, the names of the parties to the conversation and other identifying information, and the duration of each session.

INTERNET CONNECTION RECORDS: Temporarily assigned network address; Internet Protocol address;[31] dial-up telephone numbers.

## Court orders

The most common means of obtaining subscriber and transaction records is by a court order known as a "2703(d) order" or simply a "D-order."[32] The reason D-orders are popular is that they are fairly easy to prepare, the level of proof is low, and the required procedure is not complicated.

THE APPLICATION: The application for a D-order, like one for a search warrant, must include an affidavit. But it's an abbreviated affidavit and, more importantly, does not require probable cause.

Instead, the application need only demonstrate "reasonable grounds" to believe the records "are relevant and material to an ongoing criminal investigation."[33] What is required here, according to the U.S. Department of Justice, is "a short factual summary of the investigation and the role that the records will serve in advancing the investigation."[34] This summary may be contained in the application itself or in an attachment to the application.

It's important to remember that the application must contain facts—not mere conclusions. For example, in *U.S.* v. *Kennedy* an application for internet connection records in a child pornography investigation merely said the information "is relevant to an legitimate law enforcement inquiry in that it is believed that this information will assist in the investigation relating to the aforementioned offenses." In ruling this language was insufficient to support the issuance of the order, the court said:

> [T]he government should have articulated more specific facts such as how the government obtained the information it did have at the time and how this information led the agents to believe that the attainment of the subscriber information of this particular IP address would assist in the investigation.[35]

THE ORDER: Although the law does say exactly what information must be included in the order, the information required for a pen register court order should suffice, with some modifications.

DELAYED DISCLOSURE ORDER: Some communications providers are required to notify their customers that they have been ordered to release information to investigators.[36] The court may, however, instruct the provider to delay giving such notice if there is reason to believe that disclosure would, (1) endanger the life or safety of any person, (2) result in flight from prosecution, (3) result in the destruction of or tampering

---

[31] NOTE: The IP address is a number that is assigned to a computer that is connected to the internet; e.g., 128.143.7.226. See *U.S.* v. *Kennedy* (2000) 81 F.Supp.2d 1103, 1106, fn. 3 ["The IP, or Internet Protocol, address is unique to a specific computer. Only one computer would be assigned a particular IP address."].

[32] See 18 USC § 2703(d).

[33] See 18 USC §§ 2703(c)(B); 2703(d).

[34] *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).

[35] (2000) 81 F.Supp.2d 1103, 1109-10.

[36] See, for example, 6 Cal. P.U.C. 2d 421-3; Tips for Pacific Bell Response to Legal Process Feb. 14, 1995 ["Pacific Bell is required by law to notify the target of legal process that a request has been made for their records. To avoid this potentially dangerous and embarrassing situation, Pacific Bell must be ordered by the issuing court not to notify the target of your request."]

with evidence, (4) result in intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or unduly delay a trial.[37] The length of the delay may be for whatever period the judge deems appropriate.

### Search warrants

Basic subscriber and transaction records may also be obtained by means of a search warrant.[38] In most ways, the procedure for obtaining these types of search warrants is the same as any other warrant. For example, officers must submit an affidavit that establishes probable cause to believe the records are evidence. In addition, the records must be described with reasonable particularity.

DELAYED DISCLOSURE ORDER: The delayed disclosure regulations that apply to court orders (discussed earlier) also apply to search warrants.[39]

SERVING THE SEARCH WARRANT: Technically, a search warrant directs *officers* to conduct the search. But because most providers are cooperative, (plus they don't want officers traipsing through their offices and rummaging through their files), they will usually accept service by mail or fax, locate the listed records, make copies, and arrange to have them delivered, faxed, or e-mailed to the investigating officer.

SERVICE ON OUT-OF-STATE COMPANIES: If the records are located outside California, the warrant may nevertheless be issued by a California judge if the phone company is doing business in California.[40] An out-of-state provider must furnish the records within five business days after being served, although extensions are permitted.[41]

### Emergency declaration

State and federal officers may also obtain basic subscriber and transaction records by means of an emergency declaration. Under federal law, the provider must furnish the records to a law enforcement officer if it "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[42]

## PEN REGISTERS AND CONNECTION TRAPS

While transaction records provide officers with information pertaining to communications that occurred in the past, pen registers and connection traps furnish much of the same information in real time; e.g., as the numbers are dialed, as the e-mail is sent.

What are pen registers and phone traps? A "pen register" is a device or process (such as a software application) that transmits outgoing connection data in real time. Such data ordinarily includes such things as the phone numbers being dialed on a certain phone, the e-mail addresses of the recipients of e-mail messages, addresses of web sites that are being accessed, and the dates and times that contact is made.[43]

---

[37] See 18 USC § 2705(b).
[38] See 18 USC § 2703(c)(1)(A); Penal Code § 1524.3.
[39] ALSO SEE Penal 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."].
[40] See Penal Code § 1524.2.
[41] See Penal Code § 1524.2(b)(2).
[42] See 18 USC § 2702(c)(4).
[43] See 18 USC § 3124(a), 3127(3); *Smith* v. *Maryland* (1979) 442 US 735, 736, fn.1; *United States* v. *New York Telephone Co.* (1977) 434 US 159, 161, fn.1, 167; *People* v. *Blair* (1979) 25 Cal.3d 640, 654, fn.11; *People* v. *Larkin* (1987) 194 Cal.App.3d 650, 653; *People* v. *Andrino* (1989) 210 Cal.App.3d 1395, 1399, fn.2.

A connection trap provides the same information as a pen register except it records *incoming* connection data; e.g., the telephone numbers or e-mail addresses of the person who initiated the communication with the target. [44] A phone trap is akin to the "Caller ID" system.[45] Both pen registers and connection traps are ordinarily installed or programmed by the provider at its own facilities.

It should be noted that, in the past, pen registers and traps were defined as devices that acquired only telephone data. But because of developments in alternate communications technology (especially e-mail), Congress, in enacting the USA PATRIOT Act, expanded these definitions to cover devices and software applications that can record or decode the "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[46] This was a significant change because, as one commentator observed, the law now provides officers with "virtually unlimited access to individual computers through internet addresses, e-mail addresses, computer Internet Protocol addresses and port numbers, thus detecting and decoding addresses and websites contacted through the computer."[47]

### Court orders

Officers who need data from a pen register or connection trap usually seek a court order, not a search warrant. They do this for four reasons:

(1) Probable cause is not required: A court order can be issued if the records are relevant to an ongoing criminal investigation. A search warrant requires probable cause.

(2) Longer monitoring: A court order may authorize the monitoring of pen registers and traps for 60 days at a time, while a search warrant can authorize monitoring for only 10 days at a time.[48]

(3) Simple procedure: Federal law has established a quick and easy procedure for obtaining orders for pen registers and traps.[49]

(4) Nondisclosure: Nondisclosure orders are optional with search warrants but mandatory with court orders.[50]

THE APPLICATION: A federal or state court[51] may order the installation and monitoring of pen registers and phone traps if the officer's application for the order states, (1) the applicant's name and law enforcement agency; and (2) a declaration that the information that is "likely to be obtained is relevant to an ongoing criminal investigation."[52]

---

[44] See 18 USC §§ 3124(c), 3125(d); *People* v. *Suite* (1980) 101 Cal.App.3d 680, 685-7.
[45] See Public Utilities Code § 2891(a)(1); *U.S.* v. *Fregoso* (8th Cir. 1995) 60 F.3d 1314.
[46] See 18 USC §§ 3127(3) [pen registers]; 3127(4) [phone traps].
[47] *Pen Registers and Trap and Trace Devices*, James A. Adams,, Drake University Law School (2003) [Printed in the April 2003 supplement to the United States Code Service, 18 USCS §§ 2421-3160].
[48] See 18 USC § 3123(c); *People* v. *Larkin* (1987) 194 Cal.App.3d 650, 656-7.
[49] See *In re application of the United States* (1994) 846 F.Supp. 1555, 1559 ["The procedure for obtaining authorization for a pen register is summary in nature and the requisite disclosure is perfunctory."].
[50] See 18 USC § 3123(d).
[51] See footnote 20.
[52] See 18 U.S.C. §§ 3122(b); *U.S.* v. *Thompson* (11th Cir. 1991) 936 F.2d 1249, 1250 ["The applicant must certify under oath or affirmation that the information likely to be obtained is relevant to an ongoing criminal investigation."]; *Brown* v. *Waddell* (4th Cir. 1995) 50 F.3d 285, 290 ["(T)he application for authorization to use them need only certify that the information likely to be

Such a declaration does not require an explanation as to how the information would be relevant. Instead, all that is needed is a statement that the information is relevant.[53] As the court noted in *In re application of the United States*:

> The court is not asked to "approve" the application for a pen register in the sense that the court would vouch initially for the propriety of the use of a wiretap. Congress asks the court only to confirm that the approved safety measures are observed—that is, primarily, that the responsible persons are identified and accountable if any malfeasance or misprision comes to light. . . . Undoubtedly, Congress knew that providing a court false information about the nature of an investigation is an offense which . . . is due for a more unforgiving penalty.[54]

THE ORDER: The court order must contain the following information

(1) The applicant's name and law enforcement agency.
(2) The identity, if known, of the person whose telephone, computer, or other equipment will be monitored.
(3) The identity, if known, of the person who is the "subject of the criminal investigation"; i.e., the "target."
(4) A statement of the offense under investigation.
(5) (If known) The number or other identifier of the phone or other equipment that will be monitored, and the location of the equipment.
(6) A declaration that the information that is "likely to be obtained is relevant to an ongoing criminal investigation."[55]

SEALING ORDER: All court orders for pen registers and traps are automatically sealed pending further order of the court.[56]

NONDISCLOSURE ORDER: All court orders for pen registers and traps must prohibit the electronic communications from disclosing to anyone that the order has been issued.[57]

---

obtained is relevant to an ongoing criminal investigation (rather than demonstrating probable cause"]; *In re application of the United States* (1994) 846 F.Supp. 1555, 1558-9.

[53] See *U.S.* v. *Fregoso* (8th Cir. 1995) 60 F.3d 1314, 1320 ["The judicial role in approving use of trap and trace devices is ministerial in nature because, upon a proper application being made under 18 USC § 3122, 'the court *shall* enter an ex parte order authorizing the installation' of such a device."]; *U.S.* v. *Hallmark* (10th Cir. 1990) 911 F.2d 399, 402 ["Given the lack of any legitimate expectation of privacy at stake, the extremely limited judicial review required by 18 USC § 3122 is intended merely to safeguard against purely random use of this device by ensuring compliance with the statutory requirements established by Congress."]; *Brown* v. *Waddell* (4th Cir. 1995) 50 F.3d 285, 290 ["(T)he authorization may be given on a mere finding by a competent court that the applicant has made the required certification (rather than only on a probable cause determination."]; *Pen Registers and Trap and Trace Devices*, James A. Adams,, Drake University Law School (2003) [Printed in the April 2003 supplement to the United States Code Service, 18 USCS §§ 3121 et seq. p. 123] ["Although Congress requires judicial authorization for use of a pen register or trap and trace device or process, the basis for issuance is minimal. Further, when the minimal standard is met, issuance is automatic"].

[54] (1994) 846 F.Supp. 1555, 1561.

[55] See 18 U.S.C. §§ 3122(b)(2); 3123(a)(1); 3123 (a)(2); 3123(b).

[56] See 18 USC § 3123(d)(1); *Pen Registers and Trap and Trace Devices*, James A. Adams,, Drake University Law School (2003) [Printed in the April 2003 supplement to the United States Code Service, 18 USCS §§ 2421-3160] ["(O)nce the surveillance terminates, the records are sealed unless ordered opened by the court."].

[57] See 18 USC § 3123(d)(2); *Pen Registers and Trap and Trace Devices*, James A. Adams,, Drake University Law School (2003) [Printed in the April 2003 supplement to the United States Code Service, 18 USCS §§ 2421-3160] ["Targets, of course, are not notified of the issuance of a surveillance order."].

TIME LIMITS: A court order may authorize monitoring for up to 60 days, and extensions of up to 60 days.[58] To obtain an extension, officers need only submit another application. There is no requirement that officers explain why an extension is necessary, or explain what information has been obtained to date.[59]

PROVIDER MUST COOPERATE: The order may require that employees of the electronics communications service install and monitor the pen register and phone trap, and furnish periodic reports to officers.[60]

COMPENSATION TO PROVIDER: The agency requesting installation and monitoring of a pen register or phone trap must compensate the provider for its expenses in furnishing the equipment and providing technical assistance.[61]

NO SUPPRESSION: Evidence obtained as the result of a pen register or phone trap operation cannot be suppressed on grounds that the application or order did not fully comply with the statutory requirements.[62]

PRACTICE NOTE: Officers who are planning a pen register-connection trap operation should consider seeking a D-order instead of an order for a pen register and connection trap. This is because the phone numbers and e-mail address that appear on pen register-connection trap reports may not mean much unless officers also have the subscriber information for those numbers and addresses. But subscriber information can only be obtained by means of a D-order.

So, rather than apply for both a D-order and an order for a pen register-connection trap it may be better to seek a single D-order that accomplishes both objectives; i.e. it (1) authorizes the monitoring of the pen register and connection trap, and (2) requires that the provider furnish the records of its subscribers whose phone numbers or e-mail addresses were recorded during the monitoring.

### Emergency declaration

Telephone, e-mail, and internet services will immediately install a pen register or connection trap, and immediately start providing officers with data upon receiving a declaration from an officer that such data is needed to deal with any of the following, (1) an immediate danger of death or serious bodily injury to any person, (2) conspiratorial activities characteristic of organized crime, (3) an immediate threat to a national security interest, or (4) an ongoing attack (punishable as a felony) on a protected computer.[63]

For some strange reason, however, federal law states that the person who declares the emergency must be specifically authorized to do so by the California Attorney General, certain California Department of Justice administrators, or the principal

---

[58] See 18 USC § 3123(c)(1)(2).

[59] See 18 USC § 3123(c)(2); *In re application of the United States* (1994) 846 F.Supp. 1555, 1560 ["The statute [§3123(c)(2)] excludes any requirement that an applicant for an extension set forth either the results previously obtained or an explanation for the failure to obtain results."].

[60] See 18 USC § 3124; *United States* v. *New York Telephone Co.* (1977) 434 US 159, 172. ALSO SEE *Id.* at p.175-6 ["(W)ithout the [telephone company's] assistance there is no conceivable way in which the surveillance authorized by the District Court [i.e., pen register] could have been successfully accomplished."

[61] See 18 USC §§ 3124(c), 3125(d).

[62] See *U.S.* v. *Thompson* (11th Cir. 1991) 936 F.2d 1249, 1251 ["(A) violation of the statute regulating pen registers, does not result in an unconstitutional search."].

[63] See 18 USC §§ 3125(a), 1030. ALSO SEE Public Utilities Code § 2891(d)(5) [incoming and outgoing phone numbers may be given to a law enforcement agency responding to a 911 telephone call or any other call communicating an imminent threat to life or property]. NOTE: Such operations must terminate when the information sought is obtained, when the application for a court order is denied, or when 48 hours have lapsed, whichever is earlier. See 18 USC § 3125(b).

prosecuting attorney of a county or city.[64] Unless the applicant has been so designated, or unless the applicant can quickly obtain such designation, the emergency declaration statute cannot be invoked.

As a practical matter, however, if officers notify the electronic communication service of the nature of the emergency, in most cases its employees will cooperate in whatever way necessary to abate the emergency.

[64] See 18 USC 3125(a).