Electronic Communications Searches The New California Law

A new law in California ensures that law enforcement can't snoop around your digital data without first obtaining a warrant.[1]

Effective January first, California's comprehensive Electronic Communications Privacy Act (CalECPA) became law. As the result, a search warrant is now ordinarily required to obtain copies of any electronic communication content or related data that was sent to or received by a suspect or anyone else.[2] This includes email, voicemail, text messages, subscriber information, and cell site tracking data. CalECPA also changed the required form and notice requirements of electronic communications search warrants. It accomplished all of this by adding, deleting, or modifying several sections of the Penal Code.

The consequences of these changes for law enforcement are enormous because they restrict when and how officers can obtain an entire class of information which has become crucial in many criminal investigations. They do, however, provide clarity to this important area of the law which, until now, was regulated by the federal government's disordered hodgepodge known as the Electronic Communications Privacy Act (ECPA).

One of the problems with the ECPA is that it went into effect in 1986, which was several years before electronic communications became the dominant means of personal and business contact in the United States and virtually everywhere else. As the result, it enabled officers to obtain this content and data without too much difficulty. And few people complained because most people had not yet come to view electronic communications as highly private. They do now.

As these changes were occurring, the providers of electronic communications services (especially their attorneys) were becoming more and more nervous about privacy lawsuits that might result if they continued to release this information without a search warrant. So, many of them took the position that officers must obtain a warrant for almost everything, even if the ECPA might have required only a low-level court order known as a D-Order. Moreover, many judges in California were refusing to sign D-Orders because California law did not expressly authorize them to do so. And then the Sixth and Ninth Circuits issued persuasive opinions in which they ruled that, even if the ECPA did not require a search warrant, the Fourth Amendment *did*.

Congress did, however, occasionally attempt to update the ECPA by enacting legislation such as the Stored Communications Act, the Communications Assistance for Law Enforcement Act, the Patriot Act in 2001, and the Foreign Intelligence Surveillance Amendments Act in 2008. But this legislation did not satisfactorily address the general public's concern about the privacy. So the California Legislature took the initiative and, as reported by the national news media, passed CalECPA. (It has been reported that Congress may be using CalECPA as the blueprint for a new federal privacy bill.)

In this article, we will explain the fundamentals of the new law. But first, it is important to note that it was passed by a two-thirds majority of the Legislature which means that any evidence obtained in violation of the law may be suppressed.[4] Also note that because CalECPA is more strict than ECPA, officers who comply with the California law will be in compliance with federal law.

---

[1] FindLaw.com, "Digital Searches Now Require Warrants in California" (October 14, 2015) www.findlaw.com/technologist.
[2] See Pen. Code § 1546 et seq. Also see Pen. Code § 1524.3.
[3] See Pen. Code § 638.50 et seq.
[4] See Pen. Code § 1546.4; *People v. Hull* (1995) 34 Cal.App.4th 1448, 1455; *In re Lance W.* (1985) 37 Cal.3d 873.

One other thing: the information we will discuss in this introductory article is based on our understanding of CalECPA at the time we went to press. It will take a while before the Legislature and our appellate courts resolve some of the uncertainties and dubious provisions in the law. We will, of course, report on these developments as they occur.

The New Regulations

CalECPA covers nearly every form of stored electronic communications and data about such communications that might be relevant in a criminal investigation. This includes communications and data that were stored in a physical device to which officers made a physical or electronic contact (e.g., the suspect's cell phone), and information stored in equipment owned or operated by a provider(e.g., voicemail, subscriber records).[5] It also includes real time interception of cell site location information and pen register/phone trap information.

ELECTRONIC COMMUNICATION INFORMATION: As used in CalECPA, the term "electronic communication information" includes any information *about* a communication (a.k.a. "metadata.") Examples include the names of the sender and recipient of an email or text message; the time or date the communication was created, sent, or received; the IP address of a person's computer and the websites visited by that computer including the date and time of the visit.[6] The term also includes the message and cell site location information, but these subjects will be discussed separately.

It is easy to remember the requirements for obtaining electronic communication information. That's because there is only one: Officers must obtain a search warrant.[7] (It is noteworthy, and disturbing, that the Legislature decided not to permit the warrantless release of this information when it could save a life or prevent great bodily injury.)

SUBSCRIBER INFORMATION: The term "subscriber information" means general information which the subscriber submitted to the provider in order to open or maintain an account. This includes the subscriber's name, address, phone number, email address, and "similar contact information" It also includes the length of service and the types of services utilized by the subscriber.[8]

Although CalECPA provides a definition of "subscriber information," it exempted this information from its definition of "electronic communication information."[9] So we do not know for sure what officers must do to obtain it. One possibility is that providers may release it without a warrant if it is relevant to an investigation.[10] But until this is clarified, they may require a warrant.

ELECTRONIC COMMUNICATIONS: The term "electronic communication information" also includes the spoken and written words in a communication that has been stored in an electronic communications device or in equipment owned or operated by a service provider. Because "content" was included in the definition of "electronic communication information," it can only be obtained by means of a search warrant.[11] But if officers believe they have probable cause to search for communications or data stored in a device in their custody, they may seize it and promptly seek a warrant.[12]

CELL SITE LOCATION INFORMATION: "Cell Site Location Information" (CSLI) is information that identifies the physical locations of cell towers or other sites that were utilized by a provider in transmitting information to or from a particular cell phone or other device which utilized cell sites. CSLI has become useful to law enforcement because, by knowing the locations of the cell sites which carry a suspect's messages and transmission data, officers can essentially "follow" the suspect's phone and, thereby, the suspect.

---

[5] See Pen. Code § 1546.1(a)(3).
[6] See Pen. Code § 1546(d). Also see Pen. Code § 1524.3.
[7] See Pen. Code § 1546.1(b)(1); Pen. Code § 1546(b)(2).
[8] Pen. Code § 1546(l).
[9] See Pen. Code § 1546(d) [electronic communication information "does not include subscriber information"].
[10] See Pen. Code § 1546.1(f).
[11] See Pen. Code § 1546(d) ["contents"]; Pen. Code § 1546.1(b).
[12] See *Riley v. California* (2014) __ U.S. __ [134 S.Ct. 2473, 2486].

For no apparent reason, CSLI falls into three categories: "electronic communication," "electronic communication information," and "electronic device information.[13] This seems to mean it can be obtained by means of a search warrant, exigent circumstances, or "specific consent."[14] We will discuss the term "specific consent" below in the section "Consent, probation and parole searches."

There are two types of CSLI: historical and prospective. "Historical" CSLI consists of records pertaining to cell transmissions that occurred in the past.[15] For example, if officers wanted to know if a murder suspect had been near the location where the victim's body had been found, they would seek historical data for the relevant time period.

The other type of CSLI—"prospective" information—consists of cell site data that will be obtained *after* a court issues a search warrant, or *after* officers determined that CSLI was needed because of exigent circumstances. Prospective information is usually obtained in real time, meaning it is sent directly from the provider's equipment to an investigator's computer, tablet, or cell phone. For example, if officers wanted to follow a suspect by means of cell tower transmissions (or GPS) they would seek prospective data.

One method of obtaining prospective CSLI is through equipment owned or operated by a cell phone provider. This can be accomplished by having the provider "ping" the target's phone, which means transmitting an electronic signal that instructs the phone to disclose its current location. This information is then disseminated to officers in real time or through periodic reports.[16]

CSLI can also be obtained by means of a "cell site simulator." These are mobile devices that, when near the target's phone, essentially trick it into believing that the simulator is a cell site, and that it is the closest and most powerful cell site in its vicinity. This causes the cell phone to send the phone's current location It may also do a variety of more intrustive things. For example, when we went to press, cell site simulators were a hot topic in the news media because it was alleged in a privacy lawsuit that they can intercept communications as well as data.

PEN REGISTERS AND PHONE TRAPS: A "pen register" is a device or software application that records or decodes the phone numbers that are dialed on the target's phone over a particular period of time.[16] A "phone trap" or "trap and trace device" functions like a pen register but, instead of obtaining phone numbers dialed on the target's phone, it identifies the phone numbers of devices from which calls to the phone were made.[18]

Although pen registers and phone traps serve important functions in law enforcement, it is uncertain whether officers may obtain authorization to install and monitor them via a court order, or whether a search warrant is required. That is because the Legislature passed two bills in 2015—Senate Bill 178 and Assembly Bill 929—which establish different requirements for utilizing these devices. Specifically, SB 178 requires a warrant, while AB 929 requires a court order that does not require probable cause. In fact, AB 929 requires only a officer's declaration that the data which is likely to be obtained via the pen register and/or phone trap is relevant to an ongoing criminal investigation.

Based on its analysis of these two bills, the California Department of Justice concluded that AB 929 was superseded by SB 178 which would mean that a search warrant would be required. It appears that one reason for this conclusion is that SB 178 was the bill that established the comprehensive change in the law which we discussed earlier in this article,

[13] See Pen. Code §§ 1546(c); 1546(d); Pen. Code § 1546(g).
[14] See Pen. Code § 1546.1(b); Pen. Code § 1546.1(c).
[15] See *U.S. v. Graham* (4th Cir. 2015) __ F.3d __ [2015 WL 4637931]
[16] See *People v. Barnes* (2013) 216 Cal.App.4th 1508, 1511; *U.S. v. Skinner* (6th Cir. 2012) 690 F.3d 772, 778.
[17] See Pen. Code § 638.50(b).
[18] See Pen. Code § 638.50(c).
[19] See Pen. Code § 638.52.
[20] See Pen. Code § 638.52.
[21] See Pen. Code § 638.52(d); Pen. Code § 638.52(e).

while AB 929 pertained only to pen registers and phone traps. Although the Legislature is expected to correct this oversight, it usually takes some time which means that, until then, officers may need a search warrant.

Consent, probation and parole searches

CONSENT SEARCHES: Per CalECPA, the only type of search that can be conducted pursuant to the suspect's consent is a search for "electronic device information" which is defined as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device" (i.e., CSLI).[24] But such consent must constitute "specific consent," a new type of consent discussed next under "Probation searches."

PROBATION SEARCHES: It is not clear whether officers may search a probationer's cell phone or other electronic communications device pursuant to a probation search condition that authorizes warrantless searches of property under the control of the probationer. Although the legal basis for probation searches is "consent,"[25] CalECPA requires something it calls "specific consent," which it defines as "consent provided directly to the government entity seeking information."[26] What does this mean?

It seems to mean that searches of electronic communications devices are not covered under the scope of a probation search. That is because such consent is not given "directly" to officers—it is given directly to the sentencing judge in exchange for the judge's agreement not to send the probationer directly to jail or prison. Assuming that's what "specific consent" means, it admittedly represents irrational legislative overreaching. After all, it would mean that officers may search the probationer's entire home and its contents—including documents and personal property—but not his cell phone. Why should a person's cell phone be entitled to more privacy than his home? This is a question the Legislature should be required to address.

PAROLE SEARCHES: Unlike probation searches, parole and postrelease community supervision (PRCS) searches are mandated by statute,[27] which means that officers will need a search warrant. (Again, it seems strange that, as with probationers, officers may search the parolee's entire home pursuant to the terms of parole but not his cell phone.)

Warrantless searches permitted

Although a warrant is ordinarily required to search electronics communications devices and records, CalECPA expressly authorizes the following warrantless searches:

ABANDONED DEVICES: Officers may search a cell phone if they have a good faith belief that it is lost, stolen, or abandoned. However, they must limit the search to files or other information that may help "identify, verify, or contact the owner or authorized possessor of the device."[28]

INFORMATION VOLUNTARILY DISCLOSED: Neither a search warrant nor other authorization is required to search or seize information that is voluntarily disclosed to an officer by the intended recipient of the information.[29]

CELL PHONES IN PRISONS: Although it sounds obvious, a warrant is not ordinarily required to search for records stored in a cell phone that was apparently abandoned in a state prison.[30] POV

Note: *We have three new search warrant forms that may be used to obtain electronic communications and data from the following: a communications provider, a device in police custody, and a device not in police custody; e.g., the suspect's cell phone. To obtain these forms in Microsoft Word format, send an email from a departmental email address to pov.alcoda.org.*

---

[22] See Pen. Code § 638.53(a).
[23] See Pen. Code § 638.53(b).
[24] See Pen. Code § 1546.1(c)(3).
[25] See *People v. Bravo* (1987) 43 Cal.3d 600, 608; *People v. Medina* (2008) 158 Cal.App.4th 1571, 1575.
[26] See Pen. Code § 1546(k); Pen. Code § 1546.1(c)(3).
[27] See Pen. Code § 3067(a) [standard parole]; Pen. Code § 3453(f) [PRCS].
[28] See Pen. Code § 1546.1(c)(6).
[29] See Pen. Code § 1546.1(a)(3).
[30] See Pen. Code § 1546.1(c)(7).