Chapter 33
Electronic Communications and Records Searches (CalECPA)

Generally

The California Electronic Communications Privacy Act (CalECPA): CalECPA sets forth the means by which officers may obtain electronic communications and records of such communications.[2080] CalECPA covers nearly every form of stored electronic communications and most related data that might be relevant in an 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).[2081] It also includes cell site location information. In this chapter we will also cover changes to the law pertaining to pen registers and phone traps.

Chapter structure

(1) **Obtaining Subscriber Information**
(2) **Obtaining Electronic Communication Information**
(3) **Accessing Device Contents**
(4) **Obtaining Cell Site Location Information**
(5) **Monitoring Pen Registers and Phone Traps**
(6) **Suppression of Evidence**

CalECPA search warrants: To obtain electronic communications and most records pertaining to electronic communications officers must obtain a search warrant. For information about these types of search warrants see Chapter 27 SEARCH WARRANT SPECIAL PROCEDURES (Warrants For Electronic Communications and Records).

Admissibility in court: The Court of Appeal has ruled that cell phone radio technology is not a "new" technology and, thus, an officer who was trained in the field could establish at trial the reliability of such technology and explain to the court or jury how it works.[2082]

► **Forms**: Various forms pertaining to obtaining electronic communications information and data may be viewed at www.le.alcoda.org. Click on "Forms." To receive copies via email in Microsoft Word format (which can be edited), send a request from a departmental email address to CCI@acgov.org.

Related subjects covered elsewhere

Search warrants under CalECPA: Chapter 27 SEARCH WARRANT SPECIAL PROCEDURES
Electronic audio surveillance: Chapter 34 WIRETAPS
Electronic visual surveillance: Chapter 40 ELECTRONIC SURVEILLANCE
Electronic vehicle tracking: Chapter 40 ELECTRONIC SURVEILLANCE

Obtaining Subscriber Information

Defined: "Subscriber information" consists of the subscriber's name, address, phone number, email address, or "similar contact information" which the subscriber submitted to the provider in order to open or maintain an account. Such information also includes the length of service and "the types of services used by a user or of subscriber to the service provider."[2083]

Requirements

To obtain from provider

Search warrant: May be obtained by means of a CalECPA search warrant.[2084]

Voluntary cooperation: Because subscriber information does not constitute "electronic communications information" or "electronic device information,"[2085] a provider may furnish this information to officers without court authorization.[2086]

To obtain by directly accessing the device

Search warrant: May be obtained by means of a CalECPA search warrant.[2087]

Exigent circumstances: May be obtained without a warrant if officers reasonably believed that immediate access was necessary due to an imminent danger of death of serious physical injury.[2088]

Post hoc warrant application: Within three days, officers must file with the court an application, based on facts contained in an accompanying affidavit, that sets forth the facts giving rise to the emergency. Officers may also apply for authorization for delayed notification in this manner.[2089]

Notice to target: Unless delayed notification is authorized, officers must provide the target with certain information about the search.[2090]

Abandoned devices: Officers may search the device if they have a good faith belief that it is lost, stolen, or abandoned. But they may only access the information that is necessary to identify, verify, or contact the owner or authorized possessor of the device.[2091]

Obtaining Electronic Communication Information

Defined: The term "electronic communication information" is very broad, as it includes both the content of an electronic communication (i.e., the message) and any information *about* an electronic communication. Examples of electronic communications information 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.[2092] It does not include subscriber information.[2093]

How to obtain

Search warrant: May be obtained by means of a CalECPA search warrant.[2094] Also see Chapter 27 SEARCH WARRANT SPECIAL PROCEDURES (Warrants For Electronic Communications and Records).

Court order: This information may be obtained by means of a court order issued in compliance with the requirements for monitoring pen registers and phone traps. See "Monitoring Pen Registers and Phone Traps" (Court orders), below.

Accessing Device Contents: Officers may download or otherwise access electronic communication information stored on a device that is in police custody as follows:

Search warrant: May be obtained by means of a CalECPA search warrant,[2095] or a vehicle tracing search warrant.[2096] Also see Chapter 27 SEARCH WARRANT SPECIAL PROCEDURES (Warrants For Electronic Communications and Records).

Court order: This information may be obtained by means of a court order issued in compliance with the requirements for monitoring pen registers and phone traps.[2097] See "Monitoring Pen Registers and Phone Traps" (Court orders), below.

Probation or parole search: Officers may search a cell phone or other electronic communications device if it was seized from a person who owned or possessed it if (1) the person is on parole, (2) the person is a releasee under postrelease community supervision, or (3) the person is on probation with a search condition that expressly authorizes a search of electronic communications devices.[2098]

Consent

By authorized possessor: The authorized possessor of the device expressly and directly authorized officers to access the contents.[2099]

By owner: The owner of the device may consent to a search if the device was reported lost or stolen.[2100]

Exigent circumstances: Officers reasonably believed that immediate access was necessary due to an imminent danger of death of serious physical injury,[2101] or to locate the device in order to respond to an emergency 911 call from that device.[2102]

Abandoned devices: Officers may search the device if they have a good faith belief that it is lost, stolen, or abandoned.[2103] But they may only access the information that is necessary to identify, verify, or contact the owner or authorized possessor of the device.

Cell phones found in jails and prisons: If a communications device is (1) found in the possession of a jail or prison inmate, or (2) found in a state prison or in a secure area of a jail, officers may search it.[2104] This exception does not apply to cell phones possessed by authorized visitors.

Obtaining Cell Site Location Information (CSLI)

Defined: "Cell Site Location Information" (CSLI) is information that identifies the physical locations of cell towers or other sites that were utilized by a provider to transmit information to or from a particular cell phone or other device which utilized cell sites.[2105]

Types of CSLI: There are two types of CSLI: historical and prospective.

Historical: "Historical" CSLI consists of records pertaining to cell transmissions that occurred in the past.[2106] 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.

Prospective: "Prospective" information consists of cell site data that is generated *after* officers have obtained a legal right to monitor it. For example, if officers wanted to follow a suspect by means of cell tower transmissions (or GPS) they would seek prospective data. 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.

How to obtain: CSLI falls into the category of "electronic device information" (i.e., information that reveals "the current and prior locations" of the communications device[2107]) and may therefore be obtained as follows:

Search warrant: From the provider by means of a CalECPA search warrant.[2108] See Chapter 27 SEARCH WARRANT SPECIAL PROCEDURES (Warrants For Electronic Communications and Records).

Probation and parole search of device: By directly accessing the device if (1) it is in the lawful possession of officers; and (2) the owner of the device or other person who has been authorized to possess it is (a) on parole, (2) on postrelease community supervision, or (3) on probation which contains a search condition that expressly authorizes a search of such a device.[2109]

911 tracking: The device is in the possession of officers and access is necessary to respond to an emergency 911 call from that device.[2110]

Exigent circumstances: It appears that CSLI information is included within the definition of electronic device information which, if so, would mean this information could be obtained without a warrant if officers reasonably believed that the information was necessary to prevent death or serious physical injury.[2111]

Post hoc warrant application: Within three days, officers must file with the court an application, based on facts contained in an accompanying affidavit, that sets forth the facts giving rise to the emergency. Officers may also apply for authorization for delayed notification in this manner.[2112]

Notice to target: Unless delayed notification is authorized, officers must provide the target with certain information about the search.[2113]

Monitoring Pen Registers and Phone Traps

Definitions

Pen register: A "pen register" is a device or process that records or decodes the phone numbers that were dialed on a certain phone.[2114]

Trap and trace device: A "trap and trace device"—also known as a "phone trap"—functions like a pen register but, instead of obtaining phone numbers dialed from the target's phone, it identifies the phone numbers of devices from which calls to the phone were made.[2115]

Court orders: Officers may obtain authorization to install and monitor pen registers and phone traps by means of a court order; i.e., a search warrant is not required.[2116] Such a court order may be obtained as follows:

The application: Per Penal Code § 638.52(d), the application must include the following:

(1) **Applicant**: The applicant's name and agency.

(2) **Relevant to ongoing investigation**: A statement that the information to be obtained via pen register or phone trap is relevant to an ongoing criminal investigation.

(3) **Crime under investigation**: A statement of the offense to which the information likely to be obtained is relevant to the investigation.

(4) **Probable cause**: Information that establishes probable cause to believe that the sought-after information will lead to information pertaining to most felonies and certain misdemeanors. The specific offenses are listed in the statute.[2117]

(5) **Subscriber**: The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or phone trap is to be attached.

(6) **Target of investigation**: The identity, if known, of the person who is the subject of the criminal investigation.

(7) **Phone information**: The number and, if known, physical location of the telephone line to which the pen register or phone trap is to be attached and, in the case of a phone trap, the geographic limits of the trap and trace order

(8) **Crime under investigation**: The nature of the crime under investigation and an explanation of why the information likely to be obtained by the pen register or trap and trace device is relevant to the investigation.

(9) **Oath**: An application must be given under oath.

(10) **Request for technical assistance**: The application may request that the court order contain instructions to the provider to furnish information, facilities, and technical assistance which is necessary to carry out the order.[2118]

Court order: The court order must contain the information designated (4), (5), (6), (7), and (8) under "Written application," above. In addition, if the applicant requested it, the court order must instruct the provider to furnish information, facilities, and technical assistance which is necessary to carry out the order.[2119] Unless otherwise instructed, the court order shall require the provider to furnish the applicable information "at reasonable intervals during regular business hours for the duration of the order."[2120]

Time limits: The order may authorize the installation and use of the pen register or phone trap for up to 60 days.[2121] Extension may be granted upon a new application for an order under subdivisions

if the officer shows that there is a continued probable cause that the information or items sought under this subdivision are likely to be obtained under the extension.[2122] The period of an extension shall not exceed 60 days.

Compensation: The order must state that the provider shall be reasonably compensated by the requesting law enforcement agency.[2123]

Sealing of application: The application and order for pen register or phone trap authorization is automatically sealed until the order, or any extensions to the order, expire.[2124]

Notification requirements: See Pen. Code § 638.54.

Verbal authorization: A judge may verbally authorize officers to obtain pen register or phone trap information if there is probable cause to believe that the sought-after information is necessary to prevent death or serious bodily injury.[2125] There are certain technical post-search requirements that must be met promptly after the pen register or phone trap is installed. See this endnote.[2126]

Suppression of Evidence

Suppression of electronic information: Electronic information obtained in violation of CalECPA may be suppressed because the Act was passed by a two-thirds majority of the California Legislature.[2127]

Suppression of other evidence: CalECPA indicates that the only evidence that can be suppressed is "electronic information."[2128] Thus, it appears that physical evidence or anything other than "electronic information" cannot be suppressed as the fruit of a violation.