Study G-300 October 1, 2014

Memorandum 2014-50

State and Local Agency Access to Customer Information from Communication Service Providers: California Wiretap Statute and Related Law

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which directs the Commission[1] to make recommendations to revise the statutes that govern the access of state and local government agencies to customer information from communications service providers. The revisions are intended to do all of the following:

(1) Modernize the law.
(2) Protect customers' constitutional rights.
(3) Enable state and local agencies to protect public safety.
(4) Clarify procedures.

Memorandum 2014-5 introduced the study and proposed an overall organizational plan for conducting it. The Commission approved the proposed plan.[2] This memorandum begins the third step in that plan, analysis of existing California statutes. It discusses California statutes that primarily concern governmental access to communication-related information. Statutes addressing consumer privacy more generally will be discussed in a future memorandum.

The content of the memorandum is organized as follows:

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

2. See Minutes (Feb. 2014), p. 4.

The Commission invites public input on the matters discussed in this memorandum and any other point that is relevant to this study. Any interested person or group can submit formal comment to the Commission, either in writing or at a meeting. The staff is also open to receiving informal input, and is willing to meet with any interested group.

Unless otherwise indicated, all statutory references in this memorandum are to the Penal Code.

INTERCEPTION OF COMMUNICATIONS GENERALLY

As discussed in Memorandum 2014-33, the *federal* wiretap statute (hereafter "Title III")[3] contains both prohibitions on the interception of communications and exceptions that allow for law enforcement interception pursuant to lawful process.

In California those two issues are addressed in the following acts:

- The statutory prohibitions on interception are contained in Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1 of the Penal Code. This chapter is known as the "California Invasion of Privacy Act" (hereafter "CIPA").
- The statutory provisions governing law enforcement interception pursuant to court order are primarily set out in Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1 of the Penal Code (hereafter, "California Wiretap Act").

The relevant provisions of those chapters are discussed in greater detail below.

CALIFORNIA INVASION OF PRIVACY ACT

CIPA contains a number of provisions that protect the privacy of particular types of information. Several are relevant to the current study and are discussed further below. Others are not relevant to this memorandum, because they do not involve government access to customer information from a communication service provider.[4] They are not discussed further in this memorandum.

3. 18 U.S.C. § 2510 *et seq*.

4. See Sections 632 (eavesdropping), 634 (CIPA-related trespassing), 635 (eavesdropping devices), 636 (eavesdropping on prisoner), 636.5 (interception of public safety radio service communication for criminal purpose), 637.1 (opening sealed message), 637.3-637.4 (lie detector test), 637.6 (privacy of carpooling or ridesharing information), 637.9 (privacy of commercial mailing lists), 638 (commercial use of telephone calling pattern data).

Prohibitions

Wiretapping and Interception

Section 631(a) generally prohibits wiretapping and the interception of wire communications:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. If the person has previously been convicted of a violation of this section or Section 632, 632.5, 632.6, 632.7, or 636, he or she is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

As can be seen, Section 631 actually contains three discrete prohibitions. It prohibits all of the following:

- Making an unauthorized connection to a communication wire, line, cable, or instrument.
- Reading, attempting to read, or learning the contents or meaning of a message, report, or other communication while it is "in transit or passing over" any wire, line, or cable, or while being sent or received in California. This prohibition only applies if the interception is either willful and conducted without the consent of all parties or is conducted in an "unauthorized manner."

- The use or communication of information obtained in either of the two preceding ways.[5]

Section 631(a) could reasonably be read to encompass the interception of email and other forms of modern electronic communication that are transmitted by wire. However, the staff did not find any published California appellate case that expressly addresses that issue.[6] It is also worth noting that the broad language of the provision has been largely unchanged for decades; it long preceded the advent of the Internet.[7]

The prohibitions in Section 631 are stricter than the federal prohibition of unauthorized wiretapping in Title III. Most notably, Title III contains the following exceptions that have no counterpart in Section 631:

- Title III allows interception by law enforcement with the consent of only *one* of the parties to a communication.[8]
- Title III allows a communication service provider to disclose communication content to law enforcement, if the content was "inadvertently obtained" and "pertains to the commission of a crime."[9]
- Title III permits interception of a communication as part of a lawful investigation of computer trespass.[10]

Interception of Cell and Cordless Phone Communication

There are a series of sections that prohibit the interception of calls involving a "cellular radio telephone"[11] or "cordless telephone."[12] With respect to such telephones, these provisions prohibit the following conduct:

---

5. See also Tavernetti v. Sup. Ct., 22 Cal. 3d 187, 192 (1978) ("Subdivision (a) of section 631 prescribes criminal penalties for three distinct and mutually independent patterns of conduct: intentional wiretapping, wilfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities.").
6. But see In re Google Inc. Gmail Litig., 2013 U.S. Dist. LEXIS 172784 (holding that Section 631 applies to email).
7. See, e.g., 1967 Cal. Stat. ch. 1509, § 1.
8. 18 U.S.C. § 2511(2)(c)-(d).
9. *Id.* at (3)(b)(iv).
10. *Id.* at (2)(i).
11. Section 632.5(c) ("'cellular radio telephone'" means a wireless telephone authorized by the Fededral Communications Commission to operate in the frequency bandwidth reserved for cellular radio telephones.").
12. Section 632.6(c) ("'cordless telephone' means a two-way, low power communication system consisting of two parts, a 'base' unit which connects to the public switched telephone network and a handset or 'remote' unit, that are connected by a radio link and authorized by the Federal Communications Commission to operate in the frequency bandwidths reserved for cordless telephones.").

- *Maliciously* and without the consent of all parties to the communication, intercepting or receiving a communication (or assisting in doing so).[13]
- Without the consent of all parties to the communication, intercepting or receiving *and intentionally recording* a communication (or assisting in doing so).[14]

In other words, if the communication is intercepted without recording, malice is required to trigger the prohibition. But if the intercepted communication is recorded, malice is not required — the intention to record is sufficient.

Disclosure of Telegraphic or Telephonic Messages

Section 637.1 makes it unlawful to willfully disclose the content of a "telegraphic or telephonic message" addressed to another person, without that person's permission.

Similarly, Section 637.1 prohibits willfully opening a sealed envelope enclosing a telegraphic or telephonic message addressed to another person with the intent of learning the content of the message, or fraudulently impersonating a person in order to receive a message addressed to the person, with the intent to use, detain, or destroy the message.

Although these provisions, which date back to 1872, are fairly limited in their effect, they could technically fall within the scope of our study. It is conceivable that law enforcement might ask a communication service provider to disclose the content of a telegraphic or telephone message.[15]

Disclosure by Cable or Satellite Television Company

Section 637.5 protects a range of information about the customers of cable and television satellite companies. The operators of such companies are prohibited from disclosing personally identifiable information about their customers. In addition, the section specifically limits government access to certain information:

> A satellite or cable television corporation shall not make individual subscriber information available to government agencies in the absence of legal compulsion, including, but not limited to, a court order or subpoena. If requests for information are made, a satellite or cable television corporation shall promptly notify the subscriber of the nature of the request and what government

13. Sections 632.5(a), 632.6(a).
14. Section 632.7(a).
15. See also Pub. Util. Code § 7903 (prohibiting misappropriation of content of telegraphic or telephonic communication).

agency has requested the information prior to responding unless otherwise prohibited from doing so by law.[16]

Exceptions

CIPA contains a number of exceptions to the prohibitions described above. Most of those exceptions are not relevant to our study, because they do not relate to government access to information from a communication service provider.[17] They are not otherwise discussed in this memorandum. Only a few CIPA exceptions warrant discussion, as detailed below.

General Exception for Law Enforcement Access

The only general law enforcement exception in CIPA is Section 633, which provides as follows:

> 633. Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting within the scope of his or her authority, from overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.
>
> Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by the above-named persons by means of overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.

On its face, Section 633 grandfathers whatever eavesdropping and interception authority law enforcement had prior to the enactment of CIPA, which took effect on January 1, 1968.[18] However, that exception was quickly overtaken by subsequent federal constitutional and statutory developments:

---

16. Section 637.5(c).

17. See Sections 631(b)(1)-(2) (public utility communication provider operations), 632.5(b)(1)-(2) (same), 632.6(b)(1)-(2) (same), 632.7(b)(1)-(2) (same); 631(b)(3) (correctional facility internal telephone system), 632.5(b)(3) (same), 632.6(b)(3) (same), 632.7(b)(3) (same); 633.1 (recording by airport law enforcement), 633.5 (recording by party to communication to obtain evidence of specified crimes), 633.6 (recording by domestic violence victim to prove violation of court order), 633.8 (emergency eavesdropping by law enforcement).

18. See 1967 Cal. Stat. ch. 1509.

> Although originally intended to perpetuate California's then permissive rules on police surveillance, Section 633's exception was severely limited by *Berger* and *Katz*. Those decisions restricted nonconsensual police surveillance to that performed with prior judicial authorization. Even the possibility of court-ordered surveillance was short-lived, however, for [Title III] … indirectly outlawed all nonconsensual police surveillance in California. The federal act not only requires a warrant, but also requires a state enabling statute before such electronic search warrants can be issued.[19]

Consequently, whatever authority Section 633 was intended to preserve was largely trumped by the United States Supreme Court's decisions holding that wiretapping is a search under the Fourth Amendment. The contours of those decisions were codified by Title III, which applies to the states. Under Title III, California would need to enact a statute authorizing law enforcement wiretapping and that statute must conform to the minimum requirements of Title III.

California has enacted such a statute — the California Wiretap Act — which is discussed at length below. Action pursuant to a warrant issued under the California Wiretap Act is expressly excepted from the general prohibition on wiretapping and the interception of cellular and cordless telephone calls.[20]

Other Noteworthy CIPA Exceptions

Both of the provisions that prohibit unauthorized access to telegraphic or telephonic messages contain an express exception for access pursuant to a "lawful order of a court."[21]

Similarly, the provision that prohibits a cable or satellite television company from disclosing customer information to government contains an express exception for disclosure made pursuant to "legal compulsion, including, but not limited to, a court order or subpoena."[22] If a request for information is made under that provision, the company is required to "promptly notify the subscriber of the nature of the request and what government agency has requested the information prior to responding unless otherwise prohibited from doing so by law."[23]

---

19. H. Lee Van Boven, *Electronic Surveillance in California: A Study in State Legislative Control*, 57 Cal. L. Rev. 1182, 1211-12 (1969) (footnotes omitted).
20. See Section 629.88.
21. See Sections 637, 637.1.
22. See Section 637.5(c).
23. *Id.*

Remedies

A person who violates one of the prohibitions contained in CIPA is subject to criminal penalties as specified.[24]

In addition, any person injured by a violation of CIPA may bring a civil action against the violator for the greater of $5,000 or actual damages.[25] The injured person may also seek injunctive relief.[26]

Finally, CIPA expressly provides for evidence suppression as a remedy for a violation of the general prohibition on wiretapping:

> Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.[27]

Recall, however, that the Truth-in-Evidence provision of the California Constitution limits evidence exclusion remedies:

> Right to Truth-in-Evidence. Except as provided by statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature, relevant evidence shall not be excluded in any criminal proceeding, including pretrial and post conviction motions and hearings, or in any trial or hearing of a juvenile for a criminal offense, whether heard in juvenile or adult court. Nothing in this section shall affect any existing statutory rule of evidence relating to privilege or hearsay, or Evidence Code Sections 352, 782 or 1103. Nothing in this section shall affect any existing statutory or constitutional right of the press.[28]

Consequently, Section 631(c) does not appear to provide grounds for the suppression of wiretap evidence in a criminal trial.[29] However, wiretap evidence can be suppressed at trial if it was obtained in violation of the Fourth Amendment *or the California Wiretap Act*.[30] This is discussed further below.

CALIFORNIA WIRETAP ACT

As noted above, the California Wiretap Act was enacted to comply with Title III, thereby enabling California law enforcement officials to obtain search

24. See Sections 631, 632.5, 632.6, 632.7, 637, 637.1, 637.5.
25. Section 637.2(a), (c).
26. *Id.* at (b).
27. Section 631(c). See also Section 632(d) (eavesdropping).
28. Cal. Const. art. I, § 28(f)(2).
29. See, e.g., People v. Ratekin, 212 Cal. App. 3d 1165 (1989).
30. See Section 629.72.

warrants to intercept wire and electronic communications. Unsurprisingly, the California Wiretap Act closely parallels the content and structure of Title III. It includes rules governing who may apply for an interception warrant, how to apply for a warrant, standards for the court to use in deciding whether to approve a warrant, procedures for conducting interception, notice requirements, and remedies for violation of the statute. The main features of the statute are described below.

In construing the California Wiretap Act, California courts may look to federal cases that interpret equivalent provisions of Title III.[31]

Authority to Apply for Court Order

Section 629.50(a) authorizes the Attorney General (or specified deputies and assistants) and local district attorneys (or specified designees) to make an application to a presiding judge (or other designated judge) for an order authorizing an interception of a wire or oral communication. This is consistent with language in Title III that permits action by state law enforcement, pursuant to a state statute.[32]

Application for Court Order

An application for a court order to intercept a wire, oral, or electronic communication must be made in writing, upon oath or affirmation.[33] It must include all of the following information:

- The identity of the applicant and the agency that will execute the order.[34]
- A statement that the chief executive of the applying agency (or a designee) has reviewed the application and supporting facts.[35]
- A full and complete statement of the justifying facts and circumstances, including the crime being investigated, the facilities where the communication will be intercepted, the type of communication to be intercepted, and the identity of the person whose communication will be intercepted (if known).[36]

---

31. People v. Roberts, 184 Cal. App. 4th 1149, 1166-67 (2010) ("In interpreting a state wiretap scheme, the reviewing court may look for guidance to cases under title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 United States Code sections 2510 to 2520 (federal wiretap act), which provides a comprehensive scheme for the regulation of wiretapping and electronic surveillance.") (internal quotation marks omitted).
32. See 18 U.S.C. § 2516(2).
33. Section 629.50(a). *Cf.* 18 U.S.C. § 2518(1).
34. Section 629.50(a)(1)-(2). *Cf.* 18 U.S.C. § 2518(1)(a).
35. Section 629.50(a)(3).
36. *Id*. at (a)(4). *Cf.* 18 U.S.C. § 2518(1)(b).

- A statement that conventional investigative procedures have been tried and failed, are unlikely to succeed if tried, or would be too dangerous.[37]
- The period of time during which communications would be intercepted. If the nature of the investigation is such that interception should not automatically terminate when the described communication has first been obtained, a particular description of the facts showing probable cause to believe that additional communications of the same type will continue to occur.[38]
- A statement of facts concerning all previous applications involving any of the same persons, facilities, or places specified in the new application, and the action taken by the judge on those prior applications.[39]
- An application for modification of an order may be made when there is probable cause to believe that the persons identified in the original order have started using another facility or device that is not within the scope of the original order.[40]
- If the application is for an extension of a prior order, a statement of the results obtained thus far or a reasonable explanation for the failure to obtain results.[41]

The judge may require additional testimony or documentary evidence in support of an application.[42] The judge may accept a facsimile copy of the signature of any person required to give an oath or affirmation in connection with an application.[43] The application and any resulting order are sealed by the judge.[44]

Legal Standard for Granting Authority to Intercept Communication

A judge may enter an ex parte order, as requested or modified, authorizing an interception within the court's jurisdiction, of a wire, oral, or electronic communication, if the judge finds all of the following to be true, based on the facts submitted by the applicant:

37. Section 629.50(a)(4). *Cf.* 18 U.S.C. § 2518(1)(c).
38. Section 629.50(a)(5).*Cf.* 18 U.S.C. § 2518(1)(d).
39. Section 629.50(a)(6). *Cf.* 18 U.S.C. § 2518(1)(e).
40. Section 629.50(a)(8).
41. Section 629.50(a)(7). *Cf.* 18 U.S.C. § 2518(1)(f).
42. Section 629.50(b). *Cf.* 18 U.S.C. § 2518(2).
43. Section 629.50(c).
44. Section 629.66. *Cf.* 18 U.S.C. § 2518(8)(b).

- There is probable cause for belief that an individual is committing, has committed, or is about to commit a specified serious felony offense.[45]
- There is probable cause for belief that particular communications concerning that offense will be obtained through the interception.[46]
- There is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by the named person.[47]
- Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[48]

Content of Order Granting Authority to Intercept Communication

An order granting authority to intercept a wire, oral, or electronic communication is required to state the identity of the person whose communications will be intercepted (if known), the communication facilities to be used, the type of communication to be intercepted and the criminal offense to which it relates, the identity of the intercepting agency and the person who authorized the application, and the period of time during which interception is authorized (including a statement on whether authority will automatically terminate when the first described communication is intercepted).[49]

The order can also require cooperation from the affected communication service provider and other persons, which is entitled to compensation of its reasonable expenses.[50]

A judge also has general authority to conform the order to the requirements of the U.S. Constitution and federal law.[51]

Duration and Extension

As a general rule, authorization to intercept a wire, oral, or electronic communication does not continue longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days

45. Section 629.52(a). *Cf.* 18 U.S.C. § 2518(3)(a).
46. Section 629.52(b). *Cf.* 18 U.S.C. § 2518(3)(b).
47. Section 629.52(c). *Cf.* 18 U.S.C. § 2518(3)(c).
48. Section 629.52(d). *Cf.* 18 U.S.C. § 2518(3)(d).
49. Section 629.54. *Cf.* 18 U.S.C. § 2518(4).
50. Section 629.90. *Cf.* 18 U.S.C. § 2518(4).
51. Section 629.92.

(commencing on the first day of interception or 10 days after issuance of the order, whichever comes first).[52] On application, the court can extend the authorization for one or more additional periods of the same duration.[53]

Minimization

An authorized interception must be conducted so as to "minimize the interception of communications not otherwise subject to interception."[54]

The California Wiretap Act has a specific provision detailing how to minimize interception of privileged communications. When such a communication is intercepted, the officer conducting the interception must immediately cease the interception for two minutes. The interception can then be resumed for up to 30 seconds, to determine if the privileged communication continues. If so, that process repeats until the privileged communication has ended. The recording device must be "metered" in order to authenticate that the specified interruptions occurred.[55]

That process seems well tailored to the interception of streaming content (like a telephone call). It is not clear whether, or how, it would apply to the interception of asynchronous communications like email. When the Commission reaches the stage of drafting proposed language, this may be an issue that warrants some creative attention. **Public comment on how that issue might be addressed is requested.**

Interpreter

If intercepted communications are in a language other than English, law enforcement may use an interpreter who has been trained in the requirements of the California Wiretap Act (see discussion of "Training" below).[56]

Reporting

An order authorizing interception of a wire, oral, or electronic communication shall require that the intercepting agency provide the judge with reports showing what progress has been made toward the objective of the interception and the need for continuing interception. Reports shall be filed at

52. Section 629.58. *Cf.* 18 U.S.C. § 2518(5).
53. *Id.*
54. Section 629.58.
55. Section 629.80.
56. Section 629.58.

specified intervals of no more than 10 days.[57] Periodic reports must also be submitted to the Attorney General.[58]

Emergency Exception

A person authorized to apply for an interception order may make an informal application for immediate oral approval of an interception if the authorizing judge finds all of the following:

- There are grounds on which an order could be issued.
- There is probable cause to believe that an emergency situation exists with regard to the investigation of an offense of a type for which an order could be issued.
- There is probable cause to believe that a substantial danger to life or limb justifies immediate interception before an application for an order could, with due diligence, be made and acted on.[59]

If such approval is granted, it shall be conditioned on the applicant agency filing a written application for a written order, "by midnight of the second full court day after the oral approval."[60]

Recording

The contents of intercepted communications are required to be recorded (if possible), in a form that will prevent alteration. On expiration of the period of authorization, the recordings must be made available to the judge. They are held by the court, under seal. Duplicates may be made for use by law enforcement.[61]

Inventory and Notice

Within a reasonable time (not to exceed 90 days) after an authorizing order and any extension of the order has terminated, or after a judge has denied an application for authority under the emergency exception described above, an "inventory" shall be served on the persons named in the order and on any known party to an intercepted communication.[62]

The inventory document must provide notice of the interception, including the date and period of interception, and whether any communications were actually intercepted. The judge may, in the interests of justice, also order that

57. Section 629.60. *Cf.* 18 U.S.C. § 2518(6).
58. Section 629.61.
59. Section 629.56(a). *Cf.* 18 U.S.C. § 2518(7).
60. Section 629.56(b).
61. Section 629.64. *Cf.* 18 U.S.C. § 2518(8)(a).
62. Section 629.68. *Cf.* 18 U.S.C. § 2518(8)(d).

portions of the intercepted communications, applications, and orders be made available for inspection.[63]

On an ex parte showing of good cause, a judge may postpone service of the inventory.[64]

Notice must also be given to a criminal defendant, indicating that he or she was identified as a result of an interception. Notice must be given prior to the entry of a plea. At least 10 days before trial, the defendant must be given a copy of all recorded interceptions from which evidence against the defendant was derived, along with a copy of the court order, application, and monitoring logs.[65]

Training Requirements

The Commission on Peace Officer Standards and Training, in consultation with the Attorney General, is required to establish a course of training in the legal, practical and technical aspects of intercepting wire and electronic communications. An investigative or law enforcement officer (or interpreter assistant) who will conduct an interception must be certified (and periodically recertified) as meeting minimum standards.[66]

When the Commission reaches the stage of drafting proposed legislation, it might make sense to expand the training requirement to encompass all of law governing the surveillance of electronic communications.

Use of Lawfully Intercepted Communications

A specified state law enforcement official who lawfully obtains the contents of an interception of a wire or electronic communication (or derivative evidence) can disclose those contents to another specified state law enforcement official, state judge, or federal investigative or law enforcement officer to the extent appropriate to the proper performance of official duties.[67] No other disclosure can be made (except to a grand jury).[68]

A specified state law enforcement official can use intercepted content (and derivative evidence) in the proper performance of official duties.[69] Within certain limits and with judicial approval, a law enforcement official can disclose or use

63. *Id.*
64. *Id.*
65. Section 629.70(a)-(b).
66. Section 629.94.
67. Section 629.74. *Cf.* 18 U.S.C. § 2517(1).
68. *Id.*
69. Section 629.76. *Cf.* 18 U.S.C. § 2517 (2).

intercepted communications relating to offenses other than those specified in the original order authorizing interception.[70]

Any person who lawfully received the contents of an intercepted communication or evidence derived from the interception may disclose the contents or derivative evidence while giving testimony under oath or affirmation in any criminal court or grand jury proceeding.[71]

Limitations on Use of Intercepted Communications

The contents of a lawfully intercepted communication cannot be introduced into evidence in a proceeding unless all parties receive a copy of the application, as well as the order authorizing the interception, at least 10 days before the proceeding.[72] The judge may waive the 10-day period if it was not possible to provide notice to a party in that time period and the party was not prejudiced.[73] Furthermore, the judge may make an order limiting the disclosure described above, for good cause.[74]

A privileged communication does not lose its privileged status as a consequence of being intercepted, either lawfully or unlawfully.[75]

Remedies for Violations

As discussed, the California Wiretap Act does not itself prohibit interception of communications. Such prohibitions are instead provided in CIPA. Consequently, the remedies provided in the California Wiretap Act appear to be limited to violations of the California Wiretap Act only. Such violations relate to the *procedures* specified for a lawful interception.

Suppression of Evidence

Section 629.72 provides as follows:

> Any person in any trial, hearing, or proceeding, may move to suppress some or all of the contents of any intercepted wire or electronic communications, or evidence derived therefrom, only on the basis that the contents or evidence were obtained in violation of the Fourth Amendment of the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to

70. Section 629.82. *Cf.* 18 U.S.C. § 2517 (5).
71. Section 629.78. *Cf.* 18 U.S.C. § 2517 (3).
72. Section 629.70(c). *Cf.* 18 U.S.C. § 2518(9).
73. *Id.*
74. Section 629.70(d).
75. Section 629.80. *Cf.* 18 U.S.C. § 2517(4).

review in accordance with the procedures set forth in Section 1538.5.[76]

Does the Truth-in-Evidence provision of the California Constitution preclude suppression of evidence under Section 629.72? Apparently not. The Truth-in-Evidence rule does not apply, by its own terms, to a "statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature." The California Wiretap Act, including Section 629.72, was enacted after the Truth-in-Evidence provision, by more than a two-thirds supermajority vote in each house.[77]

However, not every violation of the California Wiretap Act justifies suppression of evidence. Suppression is warranted if the violated statute "was intended to play a central role in the authorization and execution of wiretaps…."[78] The burden then shifts to the State to show that the evidence should not be suppressed, because the role of the violated statute was achieved notwithstanding the violation.[79]

Civil Action

In general, a person whose communication is intercepted, disclosed, or intentionally used in violation of the California Wiretap Act may bring a civil action seeking actual or liquidated damages, punitive damages, and attorney's fees and other litigation costs.[80]

Criminal Penalty

A person who violates the California Wiretap Act may be punished by a fine, imprisoned for not more than one year, or both.[81]

Defenses

A person has a complete defense to civil and criminal liability under the California Wiretap Act if the person acted in good faith reliance on a court

76. *Cf.* 18 U.S.C. §§ 2518(10)(a), 2515.
77. People v. Jackson, 129 Cal. App. 4th 129, 153 (2005).
78. *Jackson*, 129 Cal. App. 4th at 160. See also People v. Roberts, 184 Cal. App. 4th 1149, 1183 (2010).
79. *Id.*
80. Section 629.86. *Cf.* 18 U.S.C. § 2520.
81. Section 629.84. *Cf.* 18 U.S.C. § 2511(4)(a).

order.[82] This defense is available to a person who is lending assistance to law enforcement pursuant to court order.[83]

Statistical Reporting

The Attorney General is required to prepare an annual report to the Legislature, the Judicial Council, and the Administrative Office of the United States Courts. The report compiles specified information about the interception of wire and electronic communications under the California Wiretap Act.[84]

Sunset Provision

The California Wiretap contains a sunset provision (automatically repealing the Act on a specified date, unless the sunset date is extended or eliminated prior to the provision's operation).[85] Until recently, the sunset date was January 1, 2015. But it was just extended to January 1, 2020.[86]

STORED COMMUNICATIONS

The staff could not find any California statute that addresses all of the issues governed by the federal Stored Communications Act ("SCA").[87] (The SCA generally prohibits the disclosure of stored electronic communications, subject to a number of exceptions, which include exceptions for access by government.[88]) However, there are a small number of California code sections that address particular issues that are covered by the SCA. They are discussed below.

Foreign Corporations and Foreign Warrants

Section 1524.2(b) provides rules for the service of a California search warrant on a foreign corporation that provides "electronic communication services" ("ECS") or "remote computing services" ("RCS") (as those terms are defined in the SCA[89]), for the production of records that include customer identity, data stored by or on behalf of a customer, customer usage records, addressing information for communications, and the content of communications. There is no

82. Section 629.86. *Cf.* 18 U.S.C. § 2520(d)(1).
83. Section 629.91.
84. Section 629.62. *Cf.* 18 U.S.C. § 2519.
85. Section 629.98.
86. 2014 Cal. Stat. ch. 745; SB 35 (Pavley).
87. 18 U.S.C. § 2701 *et seq.*
88. See Memorandum 2014-33, pp. 16-29.
89. Section 1524.2(a)(1).

cause of action against a corporation for compliance with a warrant issued under this section.[90]

Section 1524.2(c) provides similar rules for a warrant issued by a court in another state that is served on a California corporation that provides ECS or RCS services to the public.

The staff could not find any California statute governing a search warrant issued by a California court for service on a California corporation. The SCA would presumably fill that gap, because it applies to the states.

Evidence of Specified Misdemeanors

Section 1524.3 requires a warrant in order to obtain noncontent customer information from a company that provides ECS or RCS services, if the purpose of the search is to obtain evidence

> showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery.[91]

Legislative history indicates that this provision was added to combat identity theft, which can involve a large number of relatively modest property crimes.[92]

Law enforcement is not required to provide notice of a warrant when proceeding under Section 1524.3.[93] In anticipation of the issuance of a warrant, law enforcement can require the service provider to preserve specified records.[94] No cause of action may be brought against a service provider for good faith compliance with a warrant issued under this section.[95]

Discussion

California's fragmented statutory approach to government access to stored communications has produced some odd inconsistencies. A warrant is required for all of the following types of access:

---

90. Section 1524(d).
91. Section 1524(a)(7).
92. Senate Public Safety Committee Analysis of SB 1980 (April 30, 2002), pp. 4-5.
93. Section 1524.3(b).
94. *Id.* at (d).
95. *Id.* at (e).

- Access by California law enforcement to information held by a foreign corporation.
- Access by law enforcement in another state to information held by a California corporation.
- Non-content information held by a California communication service provider, relating to misdemeanor property crimes.

But it appears that, under the SCA, a warrant is *not* required when California law enforcement accesses customer information from a California communication service provider.[96]

This raises some perplexing questions:

- Why should greater privacy protection be afforded to the customers of a service provider in another state (a foreign corporation) than is afforded to the customers of a California service provider?
- Why should greater barriers to access apply to law enforcement in other states than apply to law enforcement in California?
- Why should a warrant be required for access to non-content customer information relating to misdemeanor property crimes when a warrant is not required for access to communication content under the SCA?

PEN REGISTERS AND TRAP AND TRACE DEVICES

The staff did not find any California statute that specifically authorizes the use of a "pen register" or "trap and trace" device to track the numbers dialed by or to a particular telephone number. However, in the opinion of the Attorney General, a pen register or trap and trace device can be used by California law enforcement if it is authorized by a search warrant.[97]

LOCATION TRACKING

There is a CIPA provision that prohibits the use of an electronic tracking device to determine the movement of a person.[98] However, that prohibition has an exception for the lawful use of a tracking device by law enforcement.[99]

---

96. See Memorandum 2014-33, pp. 21-22 (table showing authorization required under SCA in different situations).

97. See 69 Ops. Cal. Atty. Gen. 55 (1986). See also 86 Ops. Cal. Atty. Gen. 198 (2003) ("Search warrants issued by a court and subpoenas issued either by a court or grand jury are normally available to authorize the placement of pen registers and trap and trace devices in California.").

98. Section 637.7(a).

99. *Id.* at (c).

In 2012, legislation was enacted to require a warrant when law enforcement uses a tracking device.[100] The warrant will issue when the information to be received by the tracking device relates to a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code.[101]

A tracking device warrant shall be issued for a specified period of time, not to exceed 30 days (subject to extension for good cause).[102] Notice must be given to the subject of the warrant within 10 days (subject to delay for good cause).[103]

The term "tracking device" is defined as "any electronic or mechanical device that permits the tracking of the movement of a person or object."[104] That definition is quite broad and would seem to encompass both a device installed by police and a device that is used or installed by the person being tracked (e.g., a cell phone or GPS navigation system). In other words, the term appears to be broad enough to encompass location tracking information obtained by a communication service provider (e.g., cell phone triangulation data or GPS data).

That broad interpretation of the provision is supported by the following requirement:

> The search warrant shall command the officer to execute the warrant by installing a tracking device *or serving a warrant on a third-party possessor of the tracking data*.[105]

In addition, the statute provides:

> This section shall not be construed to create a cause of action against any foreign or California corporation, its officers, employees, agents, or other specified persons *for providing location information.*[106]

Such immunity would only be required if third parties are somehow involved in the tracking process, which would be true if law enforcement is obtaining tracking data from communication service providers.

Legislative analyses of the bill that added the tracking device provisions shed further light on the proper interpretation. They seem to indicate that the Legislature intended for the new legislation to govern both police-installed

100. See 2012 Cal. Stat. ch. 818 (AB 2055 (Fuentes)).
101. Section 1524(a)(12).
102. Section 1534(b)(1).
103. *Id.* at (b)(4).
104. *Id.* at (b)(6).
105. *Id.* at (b)(1) (emphasis added).
106. Section 1524(k) (emphasis added).

tracking devices and location data extracted from a device belonging to the target of the surveillance.

For example, the Assembly Committee on Public Safety explained that the bill was a response to *U.S. v. Jones*,[107] which had recently been decided by the United States Supreme Court. The majority opinion in *Jones* only addressed the Fourth Amendment's application to a tracking device that was attached to the target's car by police (which it analyzed as a trespass). The case left unanswered questions about how the Fourth Amendment applies to non-trespassory location tracking, using information that is collected from a cell phone or other GPS device and obtained from a third party communication service provider. According to the Assembly Public Safety Committee,

> The Court [in *Jones*] did not answer the question of how it might apply the Fourth Amendment to law enforcement data collection that does not require a physical intrusion, such as where GPS or toll paying devices are installed or used by the owner and the information they produce are mined by law enforcement authorities. …
>
> This bill answers some of those open questions. This bill establishes that a warrant is required to obtain tracking-device data, *regardless of whether the data is collected by means of physical intrusion or mined by law enforcement through devices installed or used by the owner.* This bill also sets forth procedures for law enforcement to follow in order to obtain a warrant.[108]

It therefore appears that the 2012 tracking device legislation was intended to apply to location data that is obtained from a target's communication service provider.

Respectfully submitted,

Brian Hebert
Executive Director

107. 132 S. Ct. 945 (2012).
108. Assembly Public Safety Committee Analysis of AB 2055 (April 17, 2012), p. 4 (emphasis added).