Study G-300 November 25, 2015

Memorandum 2015-51

State and Local Agency Access to Customer Information from Communication Service Providers (2015 Legislation and Next Steps)

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which assigned the Commission[1] a new study:

> WHEREAS, Widespread use of 21st Century mobile and Internet-based communications technologies and services enable service providers to monitor, collect, and retain large quantities of information regarding customers, including when and with whom a customer communicates or transacts business, location data, and the content of communications; and
>
> WHEREAS, Government requests to communications service providers for customer information have increased dramatically in recent years, especially by law enforcement agencies; and
>
> WHEREAS, California statutes governing access to customer information lack clarity and uniform definitions as to the legal standard for government agencies to obtain customer information from communications service providers, and many were enacted prior to the advent of wireless mobile services and the Internet; and
>
> WHEREAS, Revising and updating these statutes is necessary to reflect modern technologies and clarify the rights and responsibilities of customers, communications service providers, and government agencies seeking access to customer information; now, therefore, be it
>
> Resolved by the Senate of the State of California, the Assembly thereof concurring, That the California Law Revision Commission shall report to the Legislature recommendations to revise statutes governing access by state and local government agencies to customer information from communications service providers in order to do all of the following:
>
> (a) Update statutes to reflect 21st Century mobile and Internet-based technologies.

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.

(b) Protect customers' constitutional rights, including, but not limited to, the rights of privacy and free speech, and the freedom from unlawful searches and seizures.

(c) Enable state and local government agencies to protect public safety.

(d) Clarify the process communications service providers are required to follow in response to requests from state and local agencies for customer information or in order to take action that would affect a customer's service, with a specific description of whether a subpoena, warrant, court order, or other process or documentation is required; and be it further

Resolved, That the Secretary of the Senate transmit copies of this resolution to the author for appropriate distribution.[2]

In 2014, the staff presented a series of memoranda analyzing the statutory and constitutional law that governs electronic surveillance by state and local agencies in California.[3] With that background research completed, the Commission was ready to begin the development of proposed legislation, consistent with the goals specified by the Legislature.

Before the Commission could begin that phase of the study, circumstances changed. Senators Mark Leno and Joel Anderson introduced Senate Bill 178. That bill proposed to enact the California Electronic Communications Privacy Act (hereafter "Cal-ECPA"). As introduced, the new law would generally require a warrant or wiretap order whenever state or local agencies access any type of electronic communication information (including content, metadata, and location tracking information).

The content of SB 178 substantially overlapped with the content of the Commission's study. This put the Commission in an awkward position, for two reasons:

(1) The Commission is prohibited from taking any position on pending legislation on topics that it has been authorized to study.[4]

2. 2013 Cal. Stat. res. ch. 115.

3. See Memoranda 2014-13 (search and seizure), 2014-21 (privacy), 2014-22 (free association and expression), 2014-32 (cell phone searches), 2014-33 (Electronic Communications Privacy Act of 1986), 2014-34 (federal privacy statutes), 2014-50 (California wiretap statute and related law), 2014-55 (California privacy statutes).

4. Gov't Code § 8288 ("No employee of the commission and no member appointed by the Governor shall, with respect to any proposed legislation concerning matters assigned to the commission for study pursuant to Section 8293, advocate the passage or defeat of the legislation by the Legislature or the approval or veto of the legislation by the Governor or appear before any committee of the Legislature as to such matters unless requested to do so by the committee or its chairperson. In no event shall an employee or member of the commission appointed by the Governor advocate the passage or defeat of any legislation or the approval or veto of any legislation by the Governor, in his or her official capacity as an employee or member.").

If it were to proceed with the development of proposed legislation while SB 178 was pending in the Legislature, the Commission might be seen as taking a position on the merits of the pending bill.

(2) Proceeding with the development of proposed legislation while SB 178 was pending could be a waste of the Commission's resources. If SB 178 were to be enacted, much of the Commission's work would be duplicative.

In light of those concerns, the Commission made the following decisions:

> The … next step in the study will be to prepare a draft tentative report that describes its findings regarding the requirements of federal and state constitutional and statutory law. The report will not include any reform recommendations or proposed legislation. On approval by the Commission, the tentative report will be circulated for public comment. After consideration of public comment, a final version of the report will be approved for submission to the Legislature and Governor.
>
> The Commission will postpone further work on proposed legislation in this study until after the end of the legislative year. In the interim, the Commission will study another topic that was assigned by Senate Concurrent Resolution 54 (Padilla) (2013), the law on government interruption of communication services.[5]

The Commission took those steps and finalized an informational report on *State and Local Agency Access to Electronic Communications: Constitutional and Statutory Requirements* (Aug. 2015).[6]

The fate of SB 178 is now known. It was passed by the Legislature and signed by the Governor. It will take effect on January 1, 2016.[7] This memorandum describes the effect of SB 178. It then discusses remaining prospects for reform. Based on the information provided in this memorandum, the Commission will need to decide how to proceed.

The content of this memorandum is organized as follows:

---

5. Minutes (Feb. 2015), p. 4.

6. This report is currently in pre-print form (i.e., it has not yet been published in the Commission's bound volumes of *Reports, Recommendations, and Studies*). It is available on the Commission's website at http://www.clrc.ca.gov/pub/Printed-Reports/Pub239-G300.pdf. For ease of reference, the report will be cited as "*Pre-Print Surveillance Report*."

7. 2015 Cal. Stat. ch. 651.

CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT

Before deciding how to proceed in developing proposed legislation for this study, it is important to understand how the new 2015 legislation changed California law.

This part of the memorandum discusses Cal-ECPA. It first describes the general effect of the new law, and then discusses key elements of the law in greater detail.

General Overview

The Commission's *Pre-Print Surveillance Report* identified a number of problems with existing law. Specifically:

- The application of the Fourth Amendment to the U.S. Constitution is not entirely settled with regard to government access to email and similar content,[8] electronic communication metadata,[9] and

8. See "Third Parties and the Fourth Amendment," *Pre-Print Surveillance Report*, pp. 6-11.
9. *Id.*

location tracking information collected from a communication service provider.[10]

- The federal Stored Communications Act[11] allows access to stored electronic communications by use of a "Section 2703(d) order." The use of a 2703(d) order does not require a showing of probable cause. Thus, it would seem to be unconstitutional in cases where the Fourth Amendment applies.[12]
- The Stored Communication Act employs an unduly complicated, confusing, and seemingly obsolete scheme for specifying the level of process required for government access to different types of stored communications (based on the defined terms "electronic communication service" and "remote computing service").[13]
- The federal statutory authority for government to collect real-time or prospective location tracking information is not settled.[14]
- Government access to electronic communications could violate constitutional privacy and free expression rights.[15]

At least with respect to action by California state and local government, Senate Bill 178 resolves all of those issues. It does so by requiring a warrant (or other Fourth Amendment compatible authority[16]) for state and local government access to *all types of electronic communication information*. This includes content, metadata, and location tracking.

The approach taken by SB 178 — requiring Fourth Amendment compliant process across the board — is consistent with the Commission's own conclusions about the requirements of existing constitutional law.[17]

Thus, the enactment of Cal-ECPA significantly simplifies the Commission's task in this study. All of the "heavy lifting" has been done, with California now having statutory requirements for government surveillance that ensure the protection of constitutional search and seizure, privacy, and free expression rights.[18] The new law also provides a greater degree of certainty for service

10. See "Location Tracking," *Pre-Print Surveillance Report*, pp. 16-17.
11. 18 U.S.C. §§ 2701-2712.
12. See "Possible Unconstitutionality of Section 2703(d) Order," *Pre-Print Surveillance Report*, pp. 59-60.
13. See "Government Interception Pursuant to Lawful Process" and "Required Legal Process," *Pre-Print Surveillance Report*, pp. 56-59.
14. See "Location Tracking," *Pre-Print Surveillance Report*, pp. 67-69.
15. See "Freedom of Expression" and "Privacy," *Pre-Print Surveillance Report*, pp. 21-48.
16. E.g., a wiretap order.
17. See "Summary of Findings," *Pre-Print Surveillance Report*, pp. 75-76 ("Consequently, in California, it appears that a warrant is generally required for state and local agency access to any type of electronic communicatioin information.").
18. One possible remaining issue, relating to the use of an administrative subpoena without notice to the person whose records are to be produced, is discussed further *infra*.

providers, who no longer need to worry that a search that is permitted by statute might nonetheless violate constitutional rights.

Protected Information

Cal-ECPA defines and protects two categories of information: electronic communication information and electronic device information. The scope of each is discussed below.

Electronic Communication Information

The term "electronic communication information" is defined to have a very broad scope. It includes:

> any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address.[19]

That definition incorporates other defined terms, which are also quite broad.[20]

Notably, the definition of "electronic communication information" expressly includes both content and metadata. The references to metadata are quite detailed, and seem to be designed to encompass virtually all types of information about a communication, including any information about the location of the sender or receiver.

The definition of "electronic communication information" expressly excludes "subscriber information."[21]

Electronic Device Information

The other class of information that is protected by Cal-ECPA is electronic device information:

---

19. Section 1546(d).

20. Section 1546(c) ("'Electronic communication' means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."), (e) ("'Electronic communication service' means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.").

21. Section 1546(*l*) ("'Subscriber information' means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.").

> "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device."[22]

The related term "electronic device" is defined as follows:

> "Electronic device" means a device that stores, generates, or transmits information in electronic form.[23]

The definition of "electronic device information" seems comprehensively broad. It appears to include any information that exists on any electronic device. Nothing in the definition limits it to end-user devices, so it probably also includes information on devices controlled by service providers (e.g., servers, routers, cell towers).

Government Access Prohibitions

Cal-ECPA provides three different prohibitions on government access to protected information:

> Except as provided in this section, a government entity shall not do any of the following:
> (1) Compel the production of or access to electronic communication information from a service provider.
> (2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
> (3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.[24]

For convenience of reference and analysis, this memorandum divides those prohibitions into two categories.

The first two prohibitions involve "indirect" access to a person's electronic information. The information is not obtained by directly extracting it from a device; it is obtained by compelling a third party to provide access.

By contrast, the third prohibition involves "direct" extraction of information from an electronic device (by physical interaction or electronic communication with the device). No third party is involved.

---

22. Section 1546(g).
23. Section 1546(f).
24. Section 1546.1(a).

Exceptions for Indirect Access to Information

Notwithstanding the two prohibitions on indirect government access to protected information,[25] government may indirectly access such information by the following methods:

> A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:
>
> (1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).
>
> (2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.
>
> (3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.
>
> (4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.[26]

The exception for a non-criminal investigative subpoena is qualified. It does not permit the use of a subpoena if such use is prohibited by other state or federal law. This is a necessary qualification, because it avoids federal preemption. As discussed in prior materials, the federal Stored Communications Act does not permit the use of a subpoena to access some types of stored electronic information.[27] If Cal-ECPA were to allow such use, it would be in direct conflict with federal law.

The exclusion of criminal investigations from the subpoena provision also makes sense. As discussed in prior memoranda, the Fourth Amendment permits the use of a subpoena to conduct an "administrative search," which the Supreme Court has distinguished from a search in a criminal case.[28]

---

25. Section 1546.1(a)(1)-(2).
26. Section 1546.1(b).
27. Most significantly, the Stored Communications Act does permit the use of a subpoena to access certain electronic communications that have been stored for 180 days or less. 18 U.S.C. § 2703(a). In addition, a subpoena cannot be used to access specified non-content information. 18 U.S.C. § 2703(c)(1).
28. See, e.g., Memorandum 2015-31, pp. 2-4, discussing City of Los Angeles v. Patel, 2015 U.S. LEXIS 4065, *16 ("Search regimes where no warrant is ever required may be reasonable where

Exceptions for Direct Access to Information

Notwithstanding the prohibition on direct government access to protected information,[29] government may directly access such information by the following methods:

> A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:
>
> (1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).
>
> (2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.
>
> (3) With the specific consent of the authorized possessor of the device.
>
> (4) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.
>
> (5) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.
>
> (6) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.[30]

When government obtains electronic device information pursuant to the emergency exception set out in paragraph (5) above, it must nonetheless obtain a warrant or order authorizing its action post hoc, within three days after it obtained the information. If the court finds that the circumstances did not justify action under the emergency exception, it shall order the immediate destruction of the information obtained by the government.[31]

'special needs . . . make the warrant and probable-cause requirement impracticable,' Skinner, 489 U. S., at 619, 109 S. Ct. 1402, 103 L. Ed. 2d 639 (quoting Griffin v. Wisconsin, 483 U. S. 868, 873, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987) (some internal quotation marks omitted)), *and where the 'primary purpose' of the searches is '[d]istinguishable from the general interest in crime control,'* Indianapolis v. Edmond, 531 U. S. 32, 44, 121 S. Ct. 447, 148 L. Ed. 2d 333 (2000). Here, we assume that the searches … serve a "special need" other than conducting criminal investigations: They ensure compliance with the recordkeeping requirement, which in turn deters criminals from operating on the hotels' premises. The Court has referred to this kind of search as an 'administrative searc[h].'") (emphasis added) (some internal quotations marks omitted).

29. Section 1546.1(a)(3).
30. Section 1546.1(c).
31. Section 1546.1(h).

Special Requirements for Issuance of Warrant

Cal-ECPA expressly requires that a warrant for electronic information satisfy all other applicable requirements of state and federal law for the issuance of a warrant:

> Any warrant for electronic information shall comply with … all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants.[32]

Consequently, any specific warrant requirements established in Cal-ECPA *supplement* general warrant law, rather than supplanting it.

For example, Cal-ECPA establishes a special requirement regarding the description of electronic information to be seized:

> The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought.[33]

Cal-ECPA also requires that a service provider authenticate information provided pursuant to a warrant:

> If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.[34]

Notice to Target of Search

Subject to certain exceptions, Cal-ECPA requires that notice be given to the identified targets of a search for electronic information, whether the search is conducted pursuant to a warrant or under the emergency exception discussed above.[35]

Notice is generally required to be given contemporaneously with execution of a warrant or, in the case of an emergency, within three days after obtaining the

32. Section 1546.1(d)(3).
33. Section 1546.1(d)(1).
34. Section 1546.1(d)(3).
35. Section 1546.2(a).

information.[36] However, Cal-ECPA permits the notice to be given by a range of methods, including first class mail. In that case, there would be some delay between the time when notice is given and when it is actually received.[37]

More significantly, delivery of notice may be delayed with the approval of the court. The court shall issue an order authorizing delay (and prohibiting a person who receives the order from informing anyone about it) if it finds that providing immediate notice would produce an adverse result. The term "adverse result" is defined as follows:

> An "adverse result" means any of the following:
> (1) Danger to the life or physical safety of an individual.
> (2) Flight from prosecution.
> (3) Destruction of or tampering with evidence.
> (4) Intimidation of potential witnesses.
> (5) Serious jeopardy to an investigation or undue delay of a trial.[38]

The period of delay is limited to the time in which notice would cause an adverse result, or 90 days, whichever is shorter.[39] However, an order delaying notice can be extended by the court for additional 90-day periods.[40]

If there is no identified target for a search warrant, the information that would normally be included in a notice to the target is instead provided to the Department of Justice, which posts it on its website.[41]

Minimization Provisions

Cal-ECPA contains provisions that protect the privacy of electronic information that is obtained by warrant but that is privileged or beyond the authorized scope of the search. They are described below.

Disposition of Unrelated Information

Information that is unrelated to the purpose of a warrant must be sealed and may not be reviewed, used, or disclosed without express court authorization.[42] In addition, a court may require that such information be "destroyed as soon as

36. *Id.*
37. *Id.*
38. Section 1546(a).
39. Section 1546.2(b)(1).
40. Section 1546.2(b)(2).
41. Section 1546.2(c).
42. Section 1546.1(d)(2).

feasible after the termination of the current investigation and any related investigations or proceedings."[43]

Special Master

When issuing a warrant or other order for access to electronic information, a court may appoint a special master.[44] The special master is "charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed."[45] Cal-ECPA does not specify how a special master is to perform that function. Presumably, the special master will screen the information obtained and decide which information to pass along to law enforcement, while sealing the rest.

The concept of appointing a special master seems to be drawn from an existing procedure that applies when a warrant is issued for a search of documentary evidence in the possession or control of a lawyer, doctor, psychotherapist, or member of the clergy.[46] In that case, the appointment of a special master is mandatory, and a specific procedure is provided.[47]

Presumably, if a Cal-ECPA warrant is issued for access to "documentary evidence" that is "in the possession or control" of a lawyer, doctor, psychotherapist, or member of the clergy, the existing procedure would apply and the appointment of a special master would be mandatory. Recall that Cal-ECPA provides that a warrant must "comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, *or imposing additional requirements on the use of search warrants.*"[48]

Voluntary Disclosure by Service Provider

Cal-ECPA expressly permits a service provider to voluntarily disclose electronic communication or subscriber information, if the disclosure is not otherwise prohibited by state or federal law.[49]

If a service provider voluntarily discloses electronic information to a government entity, there are limits on its retention and use. Unless an exception applies, a government entity may only retain information that is voluntarily

43. Section 1546.1(e)(2).
44. Section 1546.1(e)(1).
45. *Id.*
46. Section 1524(c).
47. Section 1524(c)(1)-(3).
48. Section 1546.1(d)(3).
49. Section 1546.1(f).

provided by a service provider for 90 days. After that, the information must be destroyed.[50] The information need not be destroyed if any of the following conditions are met:

(1) The sender or recipient of the "electronic communications about which information was disclosed" gives consent.[51]
(2) A court order authorizing retention is issued.[52]
(3) The information is reasonably believed to relate to child pornography.[53]

Cal-ECPA does not itself contain any limits on voluntary disclosure of customer information by a service provider. However, the federal Stored Communications Act generally prohibits service provider disclosure of electronic communications.[54] That prohibition is subject to a number of exceptions, including exceptions for voluntary disclosure in the following circumstances:

- To the addressee or intended recipient of the communication.[55]
- With the lawful consent of the originator or recipient.[56]
- The contents were inadvertently obtained and appear to pertain to the commission of a crime.[57]
- Pursuant to a good faith belief that an emergency involving danger of death or serious injury requires disclosure without delay.[58]

Remedies

Evidence obtained in violation of Cal-ECPA is subject to suppression.[59] This rule does not violate the California Constitution's "Right to Truth-in-Evidence," because SB 178 was enacted by more than a two-thirds margin in each house of the Legislature.[60]

---

50. Section 1546.1(g).
51. Section 1546.1(g)(1).
52. Section 1546.1(g)(2).
53. Section 1546.1(g)(3).
54. 18 U.S.C. § 2702(a)(1)-(3).
55. 18 U.S.C. § 2702(b)(1).
56. 18 U.S.C. § 2702 (b)(3).
57. 18 U.S.C. § 2702 (b)(7).
58. 18 U.S.C. § 2702 (b)(8).
59. Section 1546.4(a).
60. Cal. Const. art. I, § 28(f)(2) ("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

The target of a search under Cal-ECPA may petition the court to void or modify an order, warrant, or other process that violates Cal-ECPA or a constitutional right.[61] The target may also petition the court for an order to destroy information obtained in violation of Cal-ECPA or a constitutional right. A service provider or other third party served with an order, warrant or other process under Cal-ECPA has the same remedies.

In addition, the Attorney General may bring a civil action to compel compliance with the requirements of Cal-ECPA.[62]

Nothing in Cal-ECPA expressly precludes remedies provided by other law. For example, the federal[63] and state[64] wiretap laws authorize a civil action for damages for an unlawful interception. Similarly, a person who is aggrieved by a knowing or intentional violation of the Stored Communications Act may bring an action for damages and other relief.[65] If a violation of Cal-ECPA is also a violation of one of those other statutes, it should be possible to pursue the remedies provided in those other statutes.

Third Party Liability

Cal-ECPA provides:

> A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.[66]

An issue relating to the scope of that provision is discussed below.

REMAINING REFORM POSSIBILITIES

Cal-ECPA has addressed nearly all of the issues identified by the Commission in its study of electronic surveillance law. However, there are a few possible reforms that the Commission may wish to pursue. They are discussed below. The

---

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.").

61. Section 1546.4(c).
62. Section 1546.4(b).
63. 18 U.S.C. § 2520.
64. Section 637.2.
65. 18 U.S.C. § 2707(a)-(b).
66. Section 1546.4(d).

first two involve technical clean-up relating to Cal-ECPA. The remainder involve issues that were not directly addressed by Cal-ECPA.

Third Party Liability

As noted above, Cal-ECPA expressly limits the liability of a corporation that acts in compliance with lawful process:

> A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.[67]

The staff has one technical concern about that provision. It is not clear why the immunity is limited to "corporations." While most service providers are likely to be incorporated, some could be organized as another form of business entity (e.g., a limited liability company). It is also possible that Cal-ECPA could be used to compel the production of information from a government entity that acts as a communication service provider (e.g., a state university providing Internet service to its students).

It might be possible to read Cal-ECPA's reference to "corporations" to include non-corporate entities, but the staff has not found any applicable definition or rule of construction in the Penal Code that would support that reading.

By contrast, existing Section 1524.3(d), provides a similar limitation on "provider" liability, using language that does not refer to a specific type of provider:

> No cause of action shall be brought against any provider, its officers, employees, or agents for providing information, facilities, or assistance in good faith compliance with a search warrant.

The use of "corporation" to describe the class of providers covered by Cal-ECPA's liability provision seems problematic. It at least raises the argument that the provision only applies to corporations. That would be at odds with the apparent policy of the liability provision — to create a safe harbor for entities that act pursuant to lawful process. It would probably be better to use the term "service provider," which is defined in Cal-ECPA.[68] Thus:

---

67. Section 1546.4(d).
68. Section 1546(j) ("Service provider" means a person or entity offering an electronic communication service.").

> A ~~California or foreign corporation~~ service provider, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.[69]

The staff invites public comment on whether this would be a helpful change and whether it might create new problems.

Conforming Existing Law to Cal-ECPA

It would probably be helpful to examine all of the existing California surveillance statutes to see if any revisions should be made to reflect the enactment of Cal-ECPA. The staff expects that this would be nonsubstantive technical clean-up work.

Special Master

With certain exceptions, when a search warrant is issued for "documentary evidence in the possession or under the control of" a lawyer, doctor, psychotherapist, or member of the clergy, the court is required to appoint a special master.[70] The special master conducts the search. If the target of the search objects that particular information should not be disclosed, the special master seals that information and takes it to court for a hearing. This allows for the screening of potentially privileged information, holding it back from disclosure until a court determines that it should be disclosed.

As discussed earlier, the mandatory special master rules would also apply when a warrant is issued pursuant to Cal-ECPA, assuming that the warrant seeks "documentary evidence" that is "in the possession or under the control of one" of the listed professionals.

In a prior memorandum, the staff raised the issue of whether electronic information held by a service provider on behalf of a customer (e.g., email stored on a server that is accessible to the customer using email software) would be considered to be within the customer's control for the purposes of the mandatory special master provision.[71] The memorandum noted a case in which the special master provision was held inapplicable to a report prepared by a consultant on

69. Section 1546.4(d).
70. Section 1524(c).
71. See Memorandum 2014-55, pp. 18-19.

behalf of a law firm client — the court held that the copy of the report on the consultant's premises was not in the law firm's possession or control.[72]

The staff believes that it might be helpful to expressly provide that customer electronic information held by a service provider is deemed to be documentary evidence within the control of the customer, for the purposes of the mandatory special master provision. This would make clear that a warrant seeking access to the electronic communications of an attorney, doctor, psychotherapist, or member of the clergy would be subject to the rule requiring appointment of a special master (regardless of whether the email is stored on a device within the professional's office or on a service provider's equipment — a distinction that is often immaterial and opaque to electronic communication users[73]). **The staff invites public comment on whether this would be helpful and whether it would create any new problems.**

Meaning of "Interception"

Existing law treats the "interception" of communications differently from access to stored communications.[74] An interception must be authorized by a wiretap order, which is subject to restrictions that do not apply to a general search warrant.

The additional restrictions on the use of a wiretap order are constitutionally-derived. In *Berger v. New York,*[75] the Court explained that an interception of communications is different from other types of searches, in ways that create special concerns with respect to the Fourth Amendment. Those special concerns require additional protections. For example:

- An authorized interception must not be indiscriminate. The warrant must describe with particularity the "things" (i.e., the conversations) to be seized. It is not sufficient to simply name the persons whose conversations will be intercepted. "[T]his does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized. As

72. See PSC Geothermal Services Co. v. Superior Court, 25 Cal. App. 4th 1697 (1994).

73. Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. … Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.").

74. See, e.g., Section 629.51(b) (application of wiretap statute).

75. 388 U.S. 41 (1967).

with general warrants this leaves too much to the discretion of the officer executing the order."[76]

- The period of authorized interception must not be over-long. Too long a period of authorization would be the "equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause. Prompt execution is also avoided. During such a long and continuous (24 hours a day) period the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation."[77]
- Because the success of real-time interception of communications depends on secrecy, there is no contemporaneous notice given to the target of the search, as there would be with a conventional search warrant. This lack of notice should be justified by some showing of exigent circumstances.[78]

Those concerns were directly addressed by Congress when it enacted a comprehensive wiretap statute.[79] That statute, which now applies to electronic communications as well as "wire" communications, requires the issuance of what is colloquially known as a "super-warrant" in order to authorize the interception of electronic and wire communications. The special requirements for issuing a super-warrant mitigate the concerns described in *Berger*. For example:

- A federal wiretap order must include "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates."[80] In addition, "Every order and extension thereof shall contain a provision that the authorization to intercept … shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter…."[81] These minimization requirements help to safeguard against the indiscriminate interception of communications that are beyond the particular scope authorized by the warrant.
- The period of interception is limited by statute. "Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable … and must terminate upon attainment of the authorized objective, or in any event in thirty days."[82] This also helps limit the indiscriminate

76. *Berger*, 288 U.S. at 59.
77. *Id*.
78. *Id*. at 60.
79. 18 U.S.C. § 2510 *et seq*.
80. 18 U.S.C. § 2518(4)(c).
81. *Id*. at (5).
82. *Id*.

collection of communications that are beyond the scope of authorization.

- The court must find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous…."[83] This exhaustion requirement helps to demonstrate exigent circumstances to justify the issuance of a warrant without contemporaneous notice to the subject of the warrant.
- Interception is only authorized in connection with a limited list of serious crimes.[84] This helps to mitigate all of the concerns discussed above, by limiting interception to unusually serious circumstances.

California's wiretap statute imposes parallel requirements and limitations.[85]

The concept of "interception" was fairly clear when *Berger* was decided. It necessarily involved contemporaneous access to communications while they were in progress (by either a wiretap or listening device). That clarity was lost with the advent of electronic communications. Electronic communication typically involves the creation and delivery of *copies* of message content, at some interval after the initial transmission.

This raises a potentially problematic question. If law enforcement waits some period of time before reading electronic communications that it acquires, is it "intercepting" them (in which case a wiretap order is required) or is it merely accessing stored communications (in which case a general search warrant is sufficient)?

This is not a theoretical concern. In *Bunnell v. Motion Picture Ass'n of America*[86] a federal district court in California held that the Wiretap Act did not apply where an email server was hacked so that it forwarded copies of email messages to a particular address. The court reasoned that this was not an "interception," because the hacker only read messages that had been placed into "storage:"

> In the instant case, Anderson's actions necessarily fall outside the scope of the Wiretap Act. Anderson configured the Bunnell parties' email server software so that all Plaintiffs' messages were copied and forwarded from the server to his Google email account.
>
> … As such, Anderson could have received the forwarded messages in milliseconds or days, it makes no difference. Under the

83. *Id*. at (3)(c).
84. 18 U.S.C. § 2516(1)-(2).
85. See Sections 629.50(a)(4) (particularity); 629.52(a) (limitation to specified crimes), (d) (exhaustion of alternatives); 629.58 (duration and minimization); 629.80 (minimization regarding privileged communications).
86. 567 F. Supp. 2d 1148 (C.D. Cal. 2007).

> Wiretap Act, his receipt of the messages does not constitute an "interception."[87]

That strikes the staff as a thin and easily manipulated distinction. It seems problematic to base the application of constitutionally necessary super-warrant requirements on such a narrow reading of "interception."

One possible reform would be to make clear that the term "interception" is used to describe any *prospective* access to communications, regardless of whether the messages are copied and stored before they are accessed. In other words, if government seeks authorization to access communications that have not yet occurred when surveillance begins, that would be an interception. If instead, the government requests access to communications that were completed prior to beginning surveillance, that would be a request for access to stored communications.

Such a distinction would track reasonably well with all of the special issues that are presented by interception (discussed above), ensuring that the specially tailored procedural rules apply whenever such issues arise.

One possible objection to enacting a statutory definition of "interception" is that it might be preempted by federal law, to the extent that it would lead to different results. However, federal law in this area does not preempt state laws that are more protective of privacy than federal law.[88]

If a definition of "interception" along the lines described above were enacted, it would seem to provide greater protection of privacy than the federal statute. That is because it would apply the "super-warrant" requirements to some borderline cases where it could be argued that a communication was "stored" before being accessed and therefore not acquired through an interception (e.g., the forwarded email copies at issue in *Bunnell*). The staff does not see any situation in which the proposed definition of "interception" would narrow the application of the super-warrant requirements.

The staff invites public comment on the preemption issue and on the merits of the proposed reform generally.

Notice of Investigative Subpoena

A warrant is not the only constitutionally-sufficient authority to conduct a search that is governed by the Fourth Amendment and Article I, Section 13 of the

87. *Id.* at 1153-54.
88. See Memorandum 2014-33, pp. 38-45.

California Constitution. The use of an investigative subpoena *duces tecum* to compel the production of evidence, for purposes other than a criminal investigation, does not violate the Fourth Amendment, so long as the subpoena is authorized, sufficiently definite, and reasonable.[89]

Consistent with that principle, Cal-ECPA permits the use of a non-criminal investigative subpoena to indirectly obtain electronic information (so long as use of the subpoena does not violate other law).[90]

However, as discussed in prior materials,[91] there is a limitation on the constitutional use of an investigative subpoena to compel the production of records: "[T]he subject of the search must be given an opportunity for precompliance review before a neutral decisionmaker."[92] The rationale for that requirement was explained in a decision of the Fourth Circuit Court of Appeal:

> While the Fourth Amendment protects people "against unreasonable searches and seizures," it imposes a probable cause requirement only on the issuance of warrants. Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment (protecting the people against "unreasonable searches and seizures"), not by the probable cause requirement.
>
> A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion. Because this intrusion is both an immediate and substantial invasion of privacy, a warrant may be issued only by a judicial officer upon a demonstration of probable cause — the safeguard required by the Fourth Amendment.
>
> *A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.*
>
> In short, the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded. And while a

89. See Los Angeles v. Patel, 2015 U.S. LEXIS 4065. See also Brovelli v. Superior Court, 56 Cal. 2d 524, 529 (1961).
90. Section 1546.1(b)(4).
91. See "Investigative Subpoena," *Pre-Print Surveillance Report*, pp. 17-21.
92. Los Angeles v. Patel, 2015 U.S. LEXIS 4065, at *16.

> challenge to a warrant questions the actual search or seizure under the probable cause standard, a challenge to a subpoena is conducted through the adversarial process, questioning the reasonableness of the subpoena's command.[93]

Advance notice and an opportunity for judicial review before records are searched are a routine feature of the procedure for issuance and execution of an investigative subpoena *duces tecum*,[94] when the subpoena is used to search records that are held by the person whose records are to be searched. But when a subpoena is instead served on a third party service provider, to search a *customer's* records, that customer might not receive any notice of the search or an opportunity for judicial review of the constitutionality of the search. In such a situation, only the service provider would have a meaningful opportunity for judicial review of the subpoena. Often, the service provider would not be an adequate surrogate to protect the interests of the customer.

It is not clear how common it would be for customer records to be produced pursuant to an investigative subpoena, without prior notice to the customer. Even if notice is not required by statute, a service provider will often have practical incentives to provide notice to its customer before complying with an investigative subpoena that demands the production of the customer's records. For example, the production of a customer's records without notice to the customer could expose the service provider to liability for violating the customer's legally-protected privacy rights or for breaching a service agreement that promises to protect customer privacy. Nonetheless, it is possible that a service provider could comply with an investigative subpoena without notifying the affected customer.

The staff has not found any case of the United States or California Supreme Courts expressly holding that the use of an investigative subpoena *duces tecum*, without notice to the person whose records are to be searched, would violate the Fourth Amendment or Article I, Section 13 of the California Constitution.

---

93. *In re* Subpoena Duces Tecum, 228 F.3d 341, 347-48 (4th. Cir. 2000) (citations omitted) (emphasis added). See also People v. West Coast Shows, Inc., 10 Cal. App. 3d 462, 470, (1970) ("the Government Code provides an opportunity for adjudication of all claimed constitutional and legal rights before one is required to obey the command of a subpoena duces tecum issued for investigative purposes").

94. See People v. Blair, 25 Cal. 3d 640, 651 (1979) ("The issuance of a subpoena duces tecum [by a grand jury] pursuant to section 1326 of the Penal Code … is purely a ministerial act and does not constitute legal process in the sense that it entitles the person on whose behalf it is issued to obtain access to the records described therein until a judicial determination has been made that the person is legally entitled to receive them."); Gov't Code § 11188 (judicial hearing to review and enforce administrative subpoena).

However, that conclusion could be drawn from the cases that explain why the use of a subpoena is constitutionally permissible.

For that reason, it might be appropriate to revise general law on the use of an investigative subpoena, for purposes other than criminal investigation, to require that notice be given to a customer whose electronic information is the subject of the search. **The staff invites public comment on that possible reform.**

CONCLUSION

As discussed above, SB 178 addressed nearly all of the issues identified by the Commission in this study. It requires Fourth Amendment level protection of all electronic information, including both metadata and location tracking information. It largely eliminates reliance on the confusing federal statutory distinction between an "electronic communication service" and a "remote computing service." It provides for special master screening to limit law enforcement access to information that is outside the scope of a warrant.

Consequently, most of the Commission's potential work in this study has been taken off the table. The reform possibilities discussed above are limited to technical clean-up and a small number of issues that were not addressed by Cal-ECPA. **The staff believes that all of those reforms are worth pursuing, but is interested to hear from the affected stakeholder community about the proposed reforms' usefulness and practicability.**

The Commission needs to decide on its next steps in this study. One possibility would be to leave the study on the back burner for a little longer. Senate Bill 178 has just been enacted and has not yet operated. It might be prudent to wait a year or so to see how Cal-ECPA operates in practice. On the other hand, a number of the reform possibilities discussed in this memorandum fall outside of the four corners of Cal-ECPA. With regard to those reforms, there may not be a need for further delay.

How would the Commission like to proceed?

Respectfully submitted,

Brian Hebert
Executive Director

Senate Bill No. 178

CHAPTER 651

An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy.

[Approved by Governor October 8, 2015. Filed with Secretary of State October 8, 2015.]

LEGISLATIVE COUNSEL'S DIGEST

SB 178, Leno. Privacy: electronic communications: search warrant.

(1) Existing law provides that a search warrant may only be issued upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing, or things and the place to be searched. Existing law also states the grounds upon which a search warrant may be issued, including, among other grounds, when the property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony, or when there is a warrant to arrest a person.

This bill would prohibit a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions, except for emergency situations, as defined. The bill would also specify the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, or consent of the owner of the device. The bill would define a number of terms for those purposes, including, among others, "electronic communication information" and "electronic device information," which the bill defines collectively as "electronic information." The bill would require a search warrant for electronic information to describe with particularity the information to be seized and would impose other conditions on the use of the search warrant or wiretap order and the information obtained, including retention, sealing, and disclosure. The bill would require a warrant directed to a service provider to be accompanied by an order requiring the service provider to verify by affidavit the authenticity of electronic information that it produces, as specified. The bill would authorize a service provider to voluntarily disclose, when not otherwise prohibited by state or federal law, electronic communication information or subscriber information, and would require a government entity to destroy information so provided within 90 days, subject to specified exceptions. The bill would, subject to exceptions, require a government entity that executes a search

warrant pursuant to these provisions to contemporaneously provide notice, as specified, to the identified target, that informs the recipient that information about the recipient has been compelled or requested, and that states the nature of the government investigation under which the information is sought. The bill would authorize a delay of 90 days, subject to renewal, for providing the notice under specified conditions that constitute an emergency. The bill would require the notice to include a copy of the warrant or statement describing the emergency under which the notice was delayed. The bill would provide that any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of its provisions, according to specified procedures. The bill would provide that a California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, wiretap order, or other order issued pursuant to these provisions.

(2) The California Constitution provides for the Right to Truth in Evidence, which requires a ⅔ vote of the Legislature to exclude any relevant evidence from any criminal proceeding, as specified.

Because this bill would exclude evidence obtained or retained in violation of its provisions in a criminal proceeding, it requires a ⅔ vote of the Legislature.

The people of the State of California do enact as follows:

SECTION 1. Chapter 3.6 (commencing with Section 1546) is added to Title 12 of Part 2 of the Penal Code, to read:

Chapter 3.6. Electronic Communications Privacy Act

1546. For purposes of this chapter, the following definitions apply:

(a) An "adverse result" means any of the following:

(1) Danger to the life or physical safety of an individual.

(2) Flight from prosecution.

(3) Destruction of or tampering with evidence.

(4) Intimidation of potential witnesses.

(5) Serious jeopardy to an investigation or undue delay of a trial.

(b) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(c) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

(d) "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication,

the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. Electronic communication information does not include subscriber information as defined in this chapter.

(e) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

(f) "Electronic device" means a device that stores, generates, or transmits information in electronic form.

(g) "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

(h) "Electronic information" means electronic communication information or electronic device information.

(i) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(j) "Service provider" means a person or entity offering an electronic communication service.

(k) "Specific consent" means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

(*l*) "Subscriber information" means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

1546.1. (a) Except as provided in this section, a government entity shall not do any of the following:

(1) Compel the production of or access to electronic communication information from a service provider.

(2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.

(b) A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.

(4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) With the specific consent of the authorized possessor of the device.

(4) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

(5) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

(6) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

(7) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility under the jurisdiction of the Department of Corrections and Rehabilitation where inmates have access and the device is not in the possession of an individual and the device is not known or believed to be the possession of an authorized visitor. Nothing in this paragraph shall be construed to supersede or override Section 4576.

(d) Any warrant for electronic information shall comply with the following:

(1) The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and

reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do any or all of the following:

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) The entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(h) If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person,

that requires access to the electronic information without delay, the entity shall, within three days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if such notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground.

(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

(3) Require a service provider to provide subscriber information.

1546.2. (a) Except as otherwise provided in this section, any government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three days after obtaining the electronic information.

(b) (1) When a warrant is sought or electronic information is obtained in an emergency under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(c) If there is no identified target of a warrant or emergency request at the time of its issuance, the government entity shall submit to the Department of Justice within three days of the execution of the warrant or issuance of the request all of the information required in subdivision (a). If an order delaying notice is obtained pursuant to subdivision (b), the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b). The department shall publish all those reports on its Internet Web site within 90 days of receipt. The department may redact names or other personal identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

1546.4. (a) Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5.

(b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter.

(c) An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.

(d) A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.

O