Study G-300 May 7, 2020

Memorandum 2020-20

State and Local Agency Access to Customer Information from Communication Service Providers (Reactivation of Study)

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, to address deficiencies identified in the Commission's study of the controlling law.

In 2015, before the Commission could begin the next phase of its work, 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 generally prohibited from taking any position on pending legislation on topics that it has been authorized to study.[4] If it had proceeded with the development of proposed

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

legislation while SB 178 was pending in the Legislature, the Commission might have been 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 have been a waste of the Commission's resources. If SB 178 were enacted, much of the Commission's work would have been 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 information-only report on *State and Local Agency Access to Electronic Communications: Constitutional and Statutory Requirements*.[6]

Later that year, SB 178 was passed by the Legislature and signed by the Governor. It took effect on January 1, 2016.[7]

Cal-ECPA accomplished nearly all of what the Commission would have recommended, had it not suspended its work on electronic surveillance. However, there were some issues at the margins that the legislation did not address. Memorandum 2015-51 described the remaining issues and sought guidance from the Commission on whether to proceed with a proposal to address those issues.

The Commission postponed pursuing those reforms at that time[8], in order to give time for the dust to settle after the enactment of Cal-ECPA. For the same reason, the work was postponed each year after that.[9]

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.").

5. Minutes (Feb. 2015), p. 4.
6. 44 Cal. L. Revision Comm'n Reports 229 (2015).
7. 2015 Cal. Stat. ch. 651.
8. Minutes (Dec. 2015), pp. 4-5.

The staff now believes that the law in this area is sufficiently settled and that the Commission should conclude its work on this study, with a narrow focus on the issues that were previously identified.

This memorandum will not reiterate the statutory and constitutional law that governs electronic communication surveillance. Commissioners who were not part of the earlier phases of this study or who need a refresher may wish to read the Commission's informational report on that topic.[10] It might also be helpful to read the part of Memorandum 2015-51 (pp. 4-15) that summarizes the effect of Cal-ECPA.

Except as otherwise indicated, statutory references in this memorandum are to the Penal Code.

SERVICE PROVIDER LIABILITY

Cal-ECPA expressly limits the liability of a California or foreign corporation that acts in compliance with an order issued pursuant to Cal-ECPA:

> 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.[11]

It is not clear why that immunity is only provided to a corporation. 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, alumni, and staff).

Cal-ECPA does not define the term "corporation." Nor is there a general definition that would apply to Cal-ECPA.

Argument in Favor of Reform

As a matter of policy, the immunity provision in Cal-ECPA should probably apply to all service providers, regardless of their form. A service provider who

---

9. See, e.g., Memorandum 2016-53, p. 8 ("Because the law is still in a state of flux, the staff recommends against reactivating the study of government access to electronic communications in 2017."); Minutes (Dec. 2016), pp. 3-4.

10. *State and Local Agency Access to Electronic Communications: Constitutional and Statutory Requirements*, 44 Cal. L. Revision Comm'n Reports 229 (2015).

11. Section 1546.4(d).

follows a lawful order that compels the disclosure of customer information should not be liable for complying with that order. If that principle applies to corporations, the staff sees no reason why it should not also apply to LLCs, partnerships, public entities, or any other form of legal entity.

Support for that argument can be found in Section 1524.3(d), a similar immunity provision that governs a warrant for the disclosure of electronic communication customer information. That subdivision provides:

> 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.

That provision applies to any *provider*, without regard to whether the provider is a corporation. That approach is consistent with the reasoning discussed above — the immunity should extend to any entity that is legally compelled to disclose customer information, regardless of the entity's form.

If that were not the case, non-corporate providers could face liability for action taken pursuant to a search warrant or other compulsory legal process. The staff sees no good argument for that result.

However, there is another provision that muddies the waters a bit. Section 1524.2 provides rules on the obligations of corporations when served with a warrant that requires the disclosure of customers' electronic communication information. The main focus of that provision is the differing obligations of California corporations and foreign corporations, when served with a warrant by a court of this state or of another state. That section includes an immunity provision that is very similar to the one used in Cal-ECPA, in that it is limited to corporations:

> (d) A cause of action shall not lie against any foreign or California corporation subject to this section, its officers, employees, agents, or other specified persons for providing records, information, facilities, or assistance in accordance with the terms of a warrant issued pursuant to this chapter.[12]

Does the existence of that provision support the idea that Cal-ECPA's immunity provision should also be limited to corporations?

12. Section 1524.2(d).

Arguably not. Section 1524.2 only regulates corporations. It therefore makes sense to limit its immunity provision to corporations; the immunity should be coextensive with the legal mandates that could otherwise cause liability.

By contrast, Cal-ECPA applies to any "person or entity offering an electronic communication service."[13] The rules are not limited to corporate entities. This means that the obligations imposed by Cal-ECPA apply to some persons and entities that are not within the scope of the immunity provision's protections. The staff sees no good policy reason for that result.

Recommendation

The staff recommends that Cal-ECPA's immunity provision be revised to apply to any "service provider," which would not be limited to corporations.[14] Thus:

> 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.[15]

Should that proposal be included in a tentative recommendation?

SPECIAL MASTER

Under Cal-ECPA, when a court issues a warrant or other order for access to electronic information, the court has *discretion* to appoint a special master.[16] The special master is "charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed."[17] 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 have been drawn from a provision outside Cal-ECPA, which applies when a warrant is issued for a search

13. Section 1546(j) ("service provider" defined).
14. Section 1546(j) ("Service provider" means a person or entity offering an electronic communication service.").
15. Section 1546.4(d).
16. Section 1546.1(e)(1).
17. *Id.*

of documentary evidence in the possession or control of a lawyer, doctor, psychotherapist, or member of the clergy "who is not reasonably suspected of engaging or having engaged in criminal activity related to the documentary evidence for which a warrant is requested."[18] In that case, the appointment of a special master is *mandatory*, and a specific procedure must be followed.[19]

The mandatory special master rule makes sense, given the heightened likelihood that records in possession of a lawyer, doctor, psychotherapist, or member of the clergy are subject to an evidentiary privilege.

Presumably, it would be good policy to apply a similar screening mechanism when a warrant seeks electronic communications of a person who meets the criteria used in the existing mandatory rule.

In fact, there is a good argument that the mandatory special master rule already applies to a search warrant issued under Cal-ECPA. That provision does not include any language expressly precluding its application to a warrant issued under Cal-ECPA.

However, there are two technical obstacles to that understanding of the mandatory special master rule.

First, the provision only applies to "documentary evidence." That term is defined broadly for the purposes of Section 1524:

> As used in this section, "documentary evidence" includes, but is not limited to, writings, documents, blueprints, drawings, photographs, computer printouts, microfilms, X-rays, files, diagrams, ledgers, books, tapes, audio and video recordings, films, and papers of any type or description.[20]

Read literally, that definition may not include electronic communications (e.g., email). However, given the close connection of this provision to the rules that govern evidentiary privileges, it seems likely that a court would construe this definition to be consistent with Evidence Code Section 250, which defines "writing" to mean (with emphasis added):

> handwriting, typewriting, printing, photostating, photographing, photocopying, *transmitting by electronic mail* or facsimile, *and every other means of recording upon any tangible thing, any form of communication or representation*, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record

18. Section 1524(c).
19. Section 1524(c)(1)-(3).
20. Section 1524(f).

> thereby created, regardless of the manner in which the record has been stored.

However, the staff did not find any case expressly construing the meaning of "documentary evidence" for the purposes of Section 1524.

It might be helpful to add language expressly providing that the term includes electronic records.

There is a second potential obstacle to applying the mandatory special master rule to a Cal-ECPA warrant: The rule only applies to documentary evidence that is "in the possession or under the control" of an attorney, doctor, psychotherapist, or member of the clergy. Is it sufficiently clear that electronic communications held on behalf of a customer by a communication service provider (e.g., email on mail server, files in cloud storage) are in the possession or under the control of the customer?

The staff found no case law directly addressing that issue. However, there is a case on the issue of possession and control when records are held by a third party. In *PSC Geothermal Services Co. v. Superior Court*,[21] the court held that the mandatory special master rule does not apply to a copy of report prepared by a consultant for an attorney, when that copy is held on the consultant's premises, because such a record is neither in the attorney's possession, nor under the attorney's control.

There might well be uncertainty as to whether the mandatory special master rule applies to electronic records that are held by a communication service provider on behalf of a customer who is an attorney, doctor, psychotherapist, or member of the clergy. Ideally, the law should be revised to eliminate that uncertainty.

The apparent policy purpose of the mandatory special master rule is to shield records that are likely to be privileged, so that they can be screened by a neutral before being passed on to law enforcement. The staff does not see any good reason for a different result if the records are in the possession of a service provider.

Suppose that Law Firm A keeps all of its files on its premises. Law Firm B keeps its records on a cloud-based storage platform provided by a third-party service provider. If the records of Law Firm A need to be screened by a special master before being disclosed pursuant to a search warrant, the same should be

21. 25 Cal. App. 4th 1697 (1994).

true of the records of Law Firm B. The records of the two firms are equally likely to contain privileged material.

It might be helpful to add language expressly providing that the mandatory special master rule applies to electronic records held by a service provider on behalf of a customer in one of the specified professions.

Would the Commission like the staff to prepare implementing language addressing the points discussed above, for inclusion in a draft tentative recommendation?

MEANING OF "INTERCEPTION" IN WIRETAP ACT

California's existing wiretap statute governs the "interception" of electronic communications. It is expressly inapplicable to "stored communications."[22] The terms "interception" and "stored communication" are not defined for the purposes of that statute.

Any confusion about the meanings of those terms could be problematic, because the requirements for a wiretap order are substantially stricter than those for a general search warrant that would be used to recover stored communications.

Super-Warrant Requirements

The stricter requirements imposed on the "interception" of communications are constitutionally-derived. In *Berger v. New York*,[23] 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 with general warrants this leaves too much to the discretion of the officer executing the order."[24]

22. See, e.g., Section 629.51(b) (application of wiretap statute).
23. 388 U.S. 41 (1967).
24. *Id*. at 59.

- The period of authorized interception must not be overlong. 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."[25]
- 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 must be justified by some showing of exigent circumstances.[26]

Those concerns were directly addressed by Congress when it enacted a comprehensive wiretap statute.[27] 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."[28] 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…."[29] 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."[30] This also helps limit the indiscriminate 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

25. *Id*.
26. *Id*. at 60.
27. 18 U.S.C. § 2510 *et seq*.
28. 18 U.S.C. § 2518(4)(c).
29. 18 U.S.C. § 2518(5).
30. *Id*.

succeed if tried or to be too dangerous…."[31] 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.[32] 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.[33]

"Interception" and Modern Electronic Communications

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 simplicity was lost with the advent of modern electronic communications. Electronic communication now typically involves the creation, delivery, and storage of *copies* of communication content, through a series of sequential steps. For example, when a person sends an email, the message content is sent from the sender's computer, to an email server, across the internet, to a destination server, and then to the recipient's computer. Copies are often retained, at least temporarily, at each step of that path.

That distinction has led some federal courts, including the Ninth Circuit, to conclude that, under the federal Wiretap Act and related statutes, the "interception" of electronic communications will almost never occur.

In *Konop v. Hawaii Airlines, Inc.*,[34] a company executive used a false identity to access a private employee website (in violation of the site's terms of service, which the executive agreed to when establishing a fraudulent account). The employee alleged, among other things, that this constituted an illegal "interception" of content in violation of the federal Wiretap Act. The court held that the executive's conduct was not an "interception" within the meaning of the Act, because interception requires that communication content "be acquired during transmission, not while it is in electronic storage."[35]

31. 18 U.S.C. § 2518(3)(c).
32. 18 U.S.C. § 2516(1)-(2).
33. 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).
34. 302 F.3d 868 (9th Cir. 2002).
35. *Id*. at 878.

Subsequent federal decisions have adopted a similarly-narrow interpretation of "interception". For example, in *Bunnell v. Motion Picture Ass'n of America*, the defendant had hacked into a computer system and configured it to forward copies of all email sent to or from a particular account. Because that forwarding happened *after* the targeted messages were sent or received, it was not an interception under the Wiretap Act.[36] Instead, it was an unauthorized access of stored communications.

> There is only a narrow window during which an E-Mail interception may occur — the seconds or milli-seconds before which a newly composed message is saved to any temporary location following a send command. … [I]nterception of E-mail within the prohibition of the Wiretap Act is virtually impossible.[37]

Courts have recognized that such a narrow construction of "interception" is "ill-suited to address modern forms of communication"[38] and may be inconsistent with Congressional intent to apply the Wiretap Act to modern forms of electronic communication. For example, under that definition of "interception," law enforcement would not need to obtain a wiretap order (i.e., a super-warrant) if it structured its surveillance along the lines used in *Bunnell*. Rather than capture email content between the sender's computer and the first server, law enforcement could simply require an email service provider to forward copies of all email 30 seconds after they are stored on the server. The substantive result would be the same as an interception, triggering all of the concerns expressed in *Berger v. New York*, but a simple warrant could apparently be used to authorize such access to "stored" communications.

Despite seeing the mismatch between the purpose of the Wiretap Act and its restrictive application to electronic communication, courts have concluded that the problem needs to be addressed legislatively.

> While Congress's definition of "intercept" does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched.[39]

---

36. 567 F. Supp. 2d 1148 (C.D. Cal. 2007).
37. United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (quoting Jarrod J. White, *E–Mail @Work.com: Employer Monitoring of Employee E–Mail*, 48 Ala. L. Rev. 1079, 1083 (1997) (brackets omitted)).
38. *Konop*, 302 F.3d at 874.
39. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003).

The Commission now has an opportunity to cover those bases, at least with regard to California's Wiretap Act.

Analysis

In the staff's view, the problem described above derives from an overly textual interpretation of interception — one that is "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.' *Webster's Ninth New Collegiate Dictionary* 630 (1985)."[40] If you access a communication after its "arrival," then you have not "intercepted" it.

A more useful approach would be to construe the Wiretap Act in terms of the purpose that it is intended to serve. Recall that the super-warrant requirements were created in response to the heightened constitutional problems that attach to interception, as explained in *Berger*.

Unlike a search for specifically-described records, an interception can be indiscriminate, overlong, and secret. To address those concerns, the Wiretap Act requires that the period of an interception be limited by the court, that minimization procedures be followed to exclude irrelevant information, that the purpose of interception be precisely defined (and limited to the investigation of serious crimes), and that a lack of practical alternatives to interception be demonstrated.

Viewed through that lens, the staff identified an alternative approach to differentiating between an interception of electronic communications and a search of stored communications. Specifically, "interception" could be defined as an action to prospectively capture communications that occur in the future (i.e., records that do not yet exist when the action is taken). Thus, the creation of a "tap" on a person's email account, designed to capture all future email sent or received by that account, would be an interception.

By contrast, an action taken to capture electronic communications that are already in existence at the time of the action would not be an interception. It would be access to stored records.

The mechanics of how electronic communications are created, transmitted, and stored would be irrelevant. The only thing would matter is whether the capture is prospective or retrospective, at the time of the action.

40. *Konop*, 302 F.3d at 878.

That approach would seem to fit nicely with the constitutional concerns discussed above. If law enforcement were to take action to prospectively capture a target's email, there would be concerns about whether the search was overbroad and overlong, and whether conducting the search without notice to the target could be justified. Imposing statutory super-warrant requirements on such a search would address those concerns.

By contrast, if law enforcement needed to search records that already existed at the time of the search, the issues raised in *Berger* would not be present. The records sought could be described with sufficient particularity to avoid overbreadth; the search would be a one-time event, avoiding overlength; and the search could be conducted with notice to the target, without foiling the purpose of the search.

Note of Caution

The staff is convinced that the prevailing interpretation of "interception" for the purposes of the federal and state Wiretap Acts is out of sync with the legislative intention to extend super-warrant requirements to the search of modern electronic communications.

The staff is not sure whether that conceptual disconnect has caused actual problems in California. It may be that California's law enforcement and courts are acting in accord with the spirit of the law, as described above. If law enforcement seeks to tap a person's email account prospectively, they may consistently be seeking a wiretap order. If a retroactive dump of prior email messages is sought, then a routine search warrant would be requested.

If that is the case, then there may not be sufficient justification to reform the law along the lines discussed above. Doing so could perhaps cause problematic unintended consequences. The term "interception" is at the heart of California's Wiretap Act. It should not be disturbed without clear need.

In light of that concern, the staff recommends that work on this issue not proceed without first gathering comment from law enforcement and judges on whether there is actually a problem. If so, it would be helpful to know whether the solution outlined above would be workable.

If instead, the Commission decides to proceed with further study of this topic, the staff would bring back draft language for inclusion in a tentative recommendation, for consideration at a future meeting.

REMAINING ISSUES

There are two other significant issues that the Commission previously considered, that could be addressed in this study:

- When a government entity seeks access to electronic communications by serving an administrative subpoena on a communication service provider, should the law require that government provide notice to the customer whose records are being sought?
- When law enforcement intercepts electronic communications that are privileged, is there some practical way to achieve the kind of minimization that Penal Code Section 629.80 requires (the temporary suspension of a wiretap when privileged communications are heard)?

The time that remains before the Commission's May meeting is not sufficient for a careful presentation of those issues. They could be discussed in a future memorandum.

NEXT STEPS

As discussed above, Cal-ECPA addressed nearly all of the issues identified by the Commission in its study of electronic surveillance, leaving only a handful of issues that might warrant reform. This memorandum begins closer examination of those issues.

The Commission should decide whether it wishes to continue study of those issues at this time (or at all). If not, the work can be set aside.

If the Commission decides to proceed with this study, the staff will do both of the following:

- Prepare a memorandum that continues work on the issues laid out in this memorandum, consistent with whatever decisions the Commission makes regarding those matters.
- Prepare a memorandum that presents the two remaining issues summarized above.

Those materials would be presented at future meetings, as time permits.

Respectfully submitted,

Brian Hebert
Executive Director