Study G-300 January 30, 2015

Memorandum 2015-3

State and Local Agency Access to Customer Information from Communication Service Providers: General Statutory Objectives

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

In conducting this study, the Commission first researched and analyzed the existing constitutional and statutory law that affects government access to such information. That work has been completed.[2]

This memorandum begins the second phase of the study — preparing proposed legislation. As a starting point, the Commission needs to make preliminary decisions on the type of legal process that should be required for state and local agency access to each of the different types of communication information at issue in this study. Once those decisions have been made, the staff can begin drafting implementing legislation.

The content of the memorandum is organized as follows:

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

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

2. See Memoranda 2014-13 (search and seizure), 2014-21 (constitutional right of privacy), 2014-22 (free expression and association), 2014-33 (federal Electronic Communications Privacy Act), 2014-34 (other federal privacy statutes), 2014-50 (California Wiretap Act and related statutory law), 2014-55 (other California privacy statutes).

LEGISLATIVE MANDATE

Senate Concurrent Resolution 54 requires the Commission to do the following:

> [T]he 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.
>
> (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; …

Subdivision (a) requires that the proposed legislation modernize the law, to reflect new and emerging communication technologies. In this memorandum, the staff will point out the opportunities for modernization that have been identified to date. **Public comment on further opportunities for modernization is invited.**

Subdivision (b) requires that the proposed law preserve existing constitutional rights, including protection against unreasonable searches and protection of the constitutional rights of privacy and free speech. The Commission will also need to be mindful of the constraints imposed by the Supremacy Clause of the United States Constitution, which could preempt the proposed legislation to the extent that it conflicts with federal statutory law.

In a sense, the requirements of subdivision (b) are self-evident. A state statute cannot contravene constitutional rights or federal statutory supremacy. Nonetheless, subdivision (b) provides strong guidance as to the Legislature's priorities in this study — constitutional rights must be protected. That express guidance may be helpful in resolving any uncertainty as to the scope of

constitutional protections in a particular scenario. It may be appropriate to err on the side of slightly overbroad protection of constitutional interests, rather than risk recommending legislation that is insufficiently protective of a constitutionally guaranteed right.

Subdivision (c) requires that the proposed law enable law enforcement to protect public safety. That requirement seems intended to caution the Commission against increasing statutory protection of privacy to such a degree as to unduly interfere with government's ability to protect the public against crime. If subdivision (b) is intended to set a constitutional "floor" on the effect of the proposed legislation, subdivision (c) may be intended to set a pragmatic "ceiling." If additional protections limit law enforcement's access to relevant evidence of crime, or impose procedural costs that consume scarce law enforcement resources, the ability of government to protect public safety could be undermined. The Commission should be mindful of that concern.

Finally, subdivision (d) requires that the proposed law provide clear procedures for use when government requests customer information from a communication service provider. Clear procedures serve two important purposes. They will help to avoid mistakes that could result in an unnecessary invasion of privacy, wasted resources, or the reversal of a conviction. Clear rules will also help to avoid the transaction costs that could result from a lack of clarity. If the requirements of the law are clear, there will be less need to consult counsel and litigate to resolve uncertainty.

The discussion that follows is informed by the legislative mandates described above.

INTERCEPTION OF COMMUNICATIONS

Existing law treats the "interception" of communications differently from access to completed communications. This makes sense because the two scenarios are materially different. Interception involves *prospective* access to communications that have not yet occurred. This introduces uncertainty as to the exact nature and scope of the communications that will be accessed. By contrast, *retrospective* access to completed communications involves a fixed set of information that can be more readily described with particularity. This should make it easier for a court to prescribe the appropriate scope of access.

In addition, prospective interception involves the following special issues:

- Interception does not involve access to records at one discrete moment in time; it occurs over a period of time.
- Interception can involve access to communication with persons who are not named in a warrant or suspected of any crime.
- Interception can involve the immediate access to communications that are privileged (without an opportunity for prior judicial review and screening).
- To be effective, interception must proceed without any advance notice to the person whose communications are being intercepted.

As discussed below, the special characteristics of prospective interception have led to special legal requirements for authorization of government access.

Constitutional and Statutory Requirements

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment protects "people, not places," meaning that the scope of its protection is not limited to physically intrusive searches. Thus, the Amendment also applies to an intangible invasion of a person's reasonable expectation of privacy (i.e., a subjective expectation of privacy that is also objectively reasonable by society's standards). This includes the interception of a conversation that is reasonably expected to be private, whether by use of a wiretap or other listening device. Consequently, a warrant is generally required for government to intercept a private communication.[3]

A regular search warrant is not sufficient for that purpose. In *Berger v. New York*, the Court explained how the special characteristics of prospective interception of communications (discussed above) create special concerns with respect to the Fourth Amendment. Those concerns must be addressed in a warrant that authorizes interception:

- The authorized interception must not be indiscriminate. The warrant must describe with particularity the place to be searched and the "things" (i.e., the conversations) to be seized. It is not

3. See Katz v. U.S., 389 U.S. 347, 361 (1967); Berger v. N.Y., 388 U.S. 41 (1967). See also Memorandum 2014-13, pp. 5-9.

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."[4]

- 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."[5]
- Because the success of real-time interception of communications depends on secrecy, there is no notice to the subject of the search, as there would be with a conventional search warrant. This should be justified by some showing of exigent circumstances.[6]

Those concerns were addressed by Congress when it enacted a comprehensive wiretap statute ("Wiretap Act").[7] 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 above. For example:

- The warrant 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."[8] 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…."[9] 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. "Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable … and must terminate

4. *Berger*, 288 U.S. at 59.
5. *Id*.
6. *Id*. at 60.
7. 18 U.S.C. § 2510 *et seq*.
8. 18 U.S.C. § 2518(4)(c).
9. *Id*. at (5).

upon attainment of the authorized objective, or in any event in thirty days."[10] This too 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 succeed if tried or to be too dangerous…."[11] 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.[12] This helps to mitigate all of the concerns discussed above, by limiting interception to unusually serious circumstances.

California's wiretap statute imposes similar requirements and limitations.[13]

What Level of Legal Process Should be Required?

As discussed above, existing law already requires a warrant before a state or local agency can intercept electronic communications. Moreover, the warrant requirement is carefully tailored to the special circumstances surrounding prospective interception. Those "super-warrant" requirements have been the law of the land for over 40 years.

In all likelihood, California law cannot provide less protection of privacy with regard to the interception of electronic or wire communications than is provided by the federal Wiretap Act. Those requirements appear to be constitutionally necessary, to address the concerns raised in *Berger v. New York*. Furthermore, the federal Wiretap Act would most likely preempt any less protective state statute.[14]

In order to protect existing constitutional rights and avoid preemption, the proposed law should continue the substance of the existing federal and California statutory super-warrant procedures with regard to the interception of electronic communications.

Opportunities for Reform

In researching the existing law governing the interception of electronic communications, the staff noted a few areas in which the law could perhaps be

10. *Id*.
11. *Id*. at (3)(c).
12. 18 U.S.C. § 2516(1)-(2).
13. Penal Code §§ 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).
14. See discussion in Memorandum 2014-33, pp. 38-45.

revised to better reflect modern communication technologies. Those possible reforms are described below.

Clarify Meaning of "Interception" of Internet-Based Communications

Internet-based communications differ from traditional wire communications in that they often involve the creation of digital copies of communication content, either temporarily as an incidental part of the transmission process, or permanently as part of an archival process. This creates some ambiguity as to the meaning of "interception."

Is the interception of an electronic communication strictly limited to access to an *original* file, as it is being transmitted? If so, could the special requirements for authorization of an interception be avoided by simply instructing a communication service provider to forward *copies* of electronic communications, at some time after the moment of transmission?

This is not a theoretical concern. In *Bunnell v. Motion Picture Ass'n of America*[15] 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 Wiretap Act, his receipt of the messages does not constitute an "interception."[16]

That strikes the staff as a thin and easily manipulated distinction. It seems problematic to base the application of the Wiretap Act's 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 to access communications that have not yet occurred at the time of authorization, that would be an interception. If instead, the government

15. 567 F. Supp. 2d 1148 (C.D. Cal. 2007).
16. *Id.* at 1153-54.

requests access to communications that were completed prior to the date of authorization, that would be a request for access to stored communications and not an interception request.

Such a distinction would track nicely 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.

Should that approach be taken in the proposed legislation?

Privileged Content in Text-Based Communications

In California, there are specific procedures for minimizing the interception of privileged communications. Penal Code Section 629.80 provides:

> No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. When a peace officer or federal law enforcement officer, while engaged in intercepting wire or electronic communications in the manner authorized by this chapter, intercepts wire or electronic communications that are of a privileged nature he or she shall immediately cease the interception for at least two minutes. After a period of at least two minutes, interception may be resumed for up to 30 seconds during which time the officer shall determine if the nature of the communication is still privileged. If still of a privileged nature, the officer shall again cease interception for at least two minutes, after which the officer may again resume interception for up to 30 seconds to redetermine the nature of the communication. The officer shall continue to go online and offline in this manner until the time that the communication is no longer privileged or the communication ends. The recording device shall be metered so as to authenticate upon review that interruptions occurred as set forth in this chapter.

That sort of time-based sampling should work well when intercepting a *streaming* communication, such as a telephone call or a videoconference. Law enforcement would simply dip in and out of the stream at the specified intervals. During the two-minute intervals when interception is suspended, the communication would not be captured, thereby preventing government access to the privileged content.

Although Section 629.80 expressly applies to the interception of "electronic communications," it is not at all clear how that would work when the content being intercepted is comprised of discrete files rather than a stream of information that can be turned off and on. For example, if law enforcement is authorized to intercept email messages that are sent or received by a particular

person, what would happen if one of the intercepted messages appears to contain some privileged content? In that situation, the requirement that law enforcement "cease the interception for at least two minutes" makes no sense. The staff does not see how existing Section 629.80 could be applied when intercepting static files. As a result, the protection of privileged communications in email, text messaging, and the like appear to be much less rigorous than the protections afforded to streaming communications.

That seems to be a significant problem, which resulted from technological change. As such, it would fall squarely within the Commission's mandate to modernize this area of the law. **Should that issue be explored further as part of this study?**

Identifying the "Facility" to be Tapped

A warrant for a wiretap must identify, with particularity, the facility that will be tapped. Before the advent of Internet-based communications, this was fairly straightforward. The facility to be tapped was a telephone, which could usually be sufficiently identified by its telephone number.[17]

Today, many cell phones are also powerful Internet-connected computers. As such, they can be used to communicate in many ways that do not involve the use of a telephone circuit. This can include forms of communication that are functionally similar to a traditional telephone call (e.g., voice-over-IP streaming audio communication) and forms that have no pre-Internet analog (e.g., email, texting, forum posting, etc.)

This multiplicity of communication channels on a single device may create practical questions about what it means to identify the "facility" that will be tapped. Is it sufficient to identify a specific communication device, in order to intercept all communications that are made with that device? Or must every type of communication be separately identified in a warrant in order for those types of communications to be intercepted?

The unprecedented technical capabilities in this area may be creating practical problems that the proposed law could help to address. **Should that issue be explored further as part of this study?**

17. J. Carr & P. Bellia, *The Law of Electronic Surveillance*, 4:25 (Aug. 2014).

Prior to the advent of the Internet, electronic communications were mostly ephemeral. There was usually no recording of the content of a telephone call. With modern electronic communications, the retention of verbatim copies of communications is often routine. Email and text messages may be stored automatically, for years, whether by the customer, the service provider, or both. This potentially creates a huge mass of searchable information about a person's private life.

Constitutional and Statutory Requirements

Fourth Amendment of the United States Constitution

The United States Supreme Court has held that there is no reasonable expectation of privacy, for the purposes of the Fourth Amendment, with regard to information that has been voluntarily revealed to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[18]

That "third party doctrine" could be understood to defeat the application of the Fourth Amendment to *any* Internet-based communication. With existing technology, virtually every electronic communication is routed through a service provider, who receives and retransmits the content of the communication. Thus, the communication has been voluntarily revealed to a third party, arguably negating any reasonable expectation of privacy as to the content of that communication.

There is one Sixth Circuit opinion that rejects that reasoning with respect to email, *United States v. Warshak*.[19] In *Warshak*, the court concluded that email is the functional equivalent of a telephone call or letter and deserving of the same Fourth Amendment protections afforded to such communication.[20] The court expressly rejected application of the third party doctrine, because an email service provider acts as a communication "intermediary," rather than the recipient of the communication.[21]

18. Smith v. Maryland, 442 U.S. 735, 742-43 (1979) (bank records). See also United States v. Miller, 425 U.S. 435 (1976) (phone numbers dialed).
19. 631 F.3d 266 (6th Cir. 2010).
20. *Id.* at 285-86.
21. *Id.* at 288.

There have also been some signals that the Supreme Court may be ready to rethink the application of the third party doctrine to electronic communications. Justice Sotomayor has expressly invited such reconsideration:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., *Smith*, 442 U. S., at 742; *United States v. Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," … and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[22]

And in the very recent case of *United States v. Riley*,[23] the Court discussed the reasonable expectation of privacy that a person has with regard to the various types of communications contained within a cell phone (including email, texts, web browsing history, and location data history). Notwithstanding the fact that all such information is voluntarily revealed to a third party, the court held that a warrant is required to search a cell phone incident to the arrest of the phone's owner. In doing so, it expressly rejected a proposed exception for call log data, which would be both easily administered and squarely within the traditional scope of the third party doctrine.

Despite those recent hints at a possible shift in thinking about the third party doctrine, there is no Supreme Court decision holding that a person has a reasonable expectation of privacy in email or other types of stored electronic communications, sufficient to trigger the application of the Fourth Amendment.

22. United States v. Jones, 132 S. Ct. 945 (2012) (Sotomayor, J. concurring).
23. 573 U.S. ___ (2014), 2014 U.S. LEXIS 4497.

Until the Court holds otherwise, it is prudent to recognize that the Fourth Amendment may not apply to electronic communications that are stored by a third party service provider.

Article I, Section 13 of the California Constitution

Article I, Section 13 of the California Constitution is largely identical in substance to the Fourth Amendment. It provides:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized.

Like the Fourth Amendment, the California Constitution's search provision rests on the existence of a reasonable expectation of privacy.[24] However, unlike the Fourth Amendment, the protections of Article I, Section 13 of the California Constitution are not limited by a third party doctrine. Under the California Constitution, the fact that a person has voluntarily revealed information to a third party for a limited purpose does not necessarily defeat the person's reasonable expectation of privacy as to that information.[25]

With regard to subjective and societal expectations of privacy, the staff sees no reason to find less of an expectation of privacy with regard to a conversation conducted using modern electronic forms of communication than exists when a conversation is conducted by telephone. However, the staff did not find any California authority directly addressing that issue. That is probably because the Internet was not in widespread use until after the "Truth-in-Evidence" provision was added to the California Constitution in 1982, by Proposition 8.[26] That provision eliminates the exclusion of evidence as a remedy for a violation of the California Constitution (with exceptions not relevant here). Consequently, there has been no reason for a criminal defendant to appeal a conviction on the ground that an Internet-based communication was obtained in violation of the California Constitution. Even if such a violation were established, the evidence would not be excluded at trial.

---

24. See, e.g., Burrows v. Superior Court, 13 Cal. 3d 238 (1974).
25. *Id.* (bank records); California v. Blair, 25 Cal. 3d 640 (1979) (phone numbers dialed; credit card usage records); People v. Chapman, 36 Cal. 3d 98 (1984) (identity associated with unlisted phone number).
26. See Cal. Const. art 1, § 28(f)(2).

However, the fact that exclusion of evidence is no longer available as a *remedy* for a violation of Article I, Section 13 does not mean that the substantive protections of that provision have been eliminated.[27] To the contrary, those protections still exist and must be taken into account. The Commission has been directed to draft legislation that protects *all* constitutional rights (without regard for the remedies that are available to redress a violation).

Based on the foregoing, the staff is fairly confident that Article I, Section 13 applies to stored electronic communications. Consequently, a warrant based on probable cause is most likely required to authorize state or local agency access to such communications.

Constitutional Right of Informational Privacy

The California Constitution includes an express provision that protects privacy,[28] which includes "informational privacy" (i.e., the interest in "precluding the dissemination or misuse of sensitive and confidential information").[29]

The United States Constitution does *not* include an express right of privacy, but certain privacy rights have been found in the penumbra of express constitutional provisions.[30] It is not clear whether these penumbral rights include a right of informational privacy.[31]

In any event, in the context of search and seizure of private information by law enforcement, the constitutional privacy right appears to be coextensive with the protection against unreasonable searches that is provided by the Fourth Amendment[32] and Article I, Section 13 of the California Constitution.[33] In other

27. *In re* Lance W., 37 Cal. 3d 873, 886-87 (1985) ("What would have been an unlawful search or seizure in this state before the passage of that initiative would be unlawful today, and this is so even if it would pass muster under the federal constitution. What Proposition 8 does is to eliminate a judicially created *remedy* for violations of the federal or state constitutions, through the exclusion of the evidence so obtained, except to the extent that exclusion remains federally compelled.").

28. Cal. Const. art. I, § 1.

29. Hill v. Nat. Collegiate Athletic Ass'n, 7 Cal. 4th 1, 35 (1994).

30. See, e.g., Griswold v. Connecticut, 381 U.S. 479, 482-84 (1965).

31. See Memorandum 2014-21, pp. 5-9, *discussing* NASA v. Nelson, 131 S. Ct. 746 (2011); Nixon v. Adm'r of Gen. Serv., 433 U.S. 425 (1977); Whalen v. Roe, 429 U.S. 589 (1977).

32. See Memorandum 2014-21, pp. 9-10, *discussing* NASA v. Nelson, 131 S. Ct. 746, 765 (2011) (Scalia, J, dissenting) ("[T]he Government's collection of private information is regulated by the Fourth Amendment, and '[w]here a particular Amendment provides an explicit textual source of constitutional protection against a particular sort of government behavior, that Amendment, not the more generalized notion of substantive due process, must be the guide for analyzing those claims.'"); County of Sacramento v. Lewis, 523 U.S. 833, 842 (1998) ("if a constitutional claim is covered by a specific constitutional provision, such as the Fourth or Eighth Amendment, the claim must be analyzed under the standard appropriate to that specific provision, not under the

words, any law enforcement search that complies with the requirements of the Fourth Amendment and Article I, Section 13 of the California Constitution will also satisfy the requirements of a constitutional right of informational privacy.

That largely obviates the need for separate analysis of the constitutional privacy right as part of this study. For the most part, this study is concerned with government access to information in connection with law enforcement. In that context, the privacy right does not provide any greater protection than the constitutional prohibition on unreasonable search and seizure.

It is possible that government could seek to access customer communication information for purposes other than law enforcement, in which case the privacy right might have independent significance. But such access is effectively precluded by existing statutory law. That law broadly protects the privacy of communications, subject only to specific statutory exceptions.[34] In the main, the exceptions that allow government access are limited to the law enforcement context.[35] Consequently, there should not be much (if any) scope for government access to communication information outside the context of a law enforcement search and seizure.

Constitutional Right of Free Expression

There are circumstances in which government access to the content of electronic communications could directly or indirectly undermine the constitutional right of free expression:

- If a person knows that his or her communications are being accessed by the government, the person might be deterred from speaking.[36]
- If a person's private associations are revealed, the person might be deterred from participating in certain groups.[37]

---

rubric of substantive due process."); Graham v. Connor, 490 U.S. 386, 395 (1989) ("Because the Fourth Amendment provides an explicit textual source of constitutional protection against this sort of physically intrusive governmental conduct, that Amendment, not the more generalized notion of 'substantive due process,' must be the guide for analyzing these claims.").

33. See Memorandum 2014-21, pp. 22-24, *discussing* People v. Crowson, 33 Cal. 3d 623, 629 (1983) ("In the search and seizure context, the article I, section 1 'privacy' clause has never been held to establish a broader protection than that provided by the Fourth Amendment of the United States Constitution or article I, section 13 of the California Constitution. '[The] search and seizure and privacy protections [are] coextensive when applied to police surveillance in the criminal context.'"); *In re* York, 9 Cal. 4th 1133 (1995) (same).
34. 18 U.S.C. §§ 2511(1)(a)-(b) (interception), 2701(a) (stored communications).
35. 18 U.S.C. §§ 2516 (interception), 2703 (stored communications).
36. See Memorandum 2014-22, pp. 20-24; White v. Davis, 13 Cal. 3d 757 (1975).

- If a person's online identity is revealed, the person's ability to speak anonymously could be defeated or deterred.[38]
- If a person's online browsing history is revealed, the right to "reader privacy" could be undermined, which could deter the person from reading certain content.[39]
- If a journalist's communications are obtained, confidential information and sources could be revealed.[40]

The concerns described above could perhaps be sufficiently addressed by making clear that a search of electronic communications must comply with the warrant requirements of the Fourth Amendment and Article I, Section 13 of the California Constitution. This would ensure that any proposed search that might affect free expression would be reviewed by a judge, who would determine whether the search is constitutionally reasonable and could thus consider any free speech interests at stake and tailor the warrant accordingly.

Support for that approach can be found in *Zurcher v. Stanford Daily*.[41] In that case, police searched a college newspaper's offices for photographs that might reveal the identity of demonstrators who had assaulted police. The *Stanford Daily* objected to the search, in part on the ground that it violated its First Amendment rights in a number of ways:

> First, searches will be physically disruptive to such an extent that timely publication will be impeded. Second, confidential sources of information will dry up, and the press will also lose opportunities to cover various events because of fears of the participants that press files will be readily available to the authorities. Third, reporters will be deterred from recording and preserving their recollections for future use if such information is subject to seizure. Fourth, the processing of news and its dissemination will be chilled by the prospects that searches will disclose internal editorial deliberations. Fifth, the press will resort to self-censorship to conceal its possession of information of potential interest to the police.[42]

---

37. See Memorandum 2014-22, pp. 5-11; National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).
38. See Memorandum 2014-22, pp. 11-15; Talley v. California, 362 US 60 (1960).
39. See Memorandum 2014-22, pp. 17-20; Stanley v. Georgia, 394 U.S. 557, 565 (1969); Lamont v. Postmaster General, 381 U.S. 301 (1965); United States v. Rumely, 345 U.S. 41 (1953). See also 18 U.S.C. § 2710 (Video Privacy Protection Act); Civ. Code §§ 1799.3 (video records), 1798.90-1798.90.05 (Reader Privacy Act).
40. See Zurcher v. Stanford Daily, 436 U.S. 547.
41. 436 U.S. 547.
42. *Id.* at 563-64.

Despite the seriousness of those concerns, the Supreme Court nonetheless held that a search of a newspaper's offices is lawful if supported by a properly-framed warrant:

> Properly administered, the preconditions for a warrant — probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness — should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices.
>
> …
>
> The hazards of such warrants can be avoided by a neutral magistrate carrying out his responsibilities under the Fourth Amendment, for he has ample tools at his disposal to confine warrants to search within reasonable limits.[43]

If a warrant requirement is the approach used in the important context of the freedom of the press, it seems likely that the same would be true of the other types of potential free expression impairment that are described above.

These considerations provide further support for applying the Fourth Amendment's protections to a government search of electronic communications.

Importantly, there are also federal and state statutory restrictions on the use of a warrant to search a journalist's records.[44] **As discussed in prior memoranda, the proposed legislation will need to preserve those existing statutory protections**.[45]

Stored Communications Act

The federal Stored Communications Act ("SCA")[46] regulates the disclosure of stored electronic communications.

For the purposes of the SCA,[47] the term "electronic communications" is defined very broadly, to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" (excluding oral or wire communications, tone only pagers, and electronic fund transfers).[48] That is broad enough to encompass

43. *Id.* at 565-67.
44. See 42 U.S.C. § 2000aa; Penal Code § 1524(g).
45. See Memorandum 2014-34, pp. 8-10; Memorandum 2014-55, p. 19.
46. 18 U.S.C. § 2701 *et seq*.
47. 18 U.S.C. § 2711(1).
48. 18 U.S.C. § 2501(12).

the full panoply of modern Internet-based communication technologies, including private social media content such as nonpublic[49] Facebook, Twitter, or discussion group postings.[50]

The SCA establishes a hierarchy of legal process requirements for government access to the content of stored electronic communications. That hierarchy is based on whether the communication is stored in an "electronic communication service" ("ECS")[51] or a "remote computing service" ("RCS"),[52] whether the communication has been stored for more than 180 days, and whether prior notice of the access is given to the customer.[53] As discussed in a prior memorandum, the 180-day storage criteria and the distinction between ECS and RCS are considered by many to be obsolete relics of an earlier technological era.[54]

The rules for access to communication content under the SCA can be summarized as follows:

- For ECS data stored 180 days or fewer, a search warrant is required.[55]
- For all other stored electronic communication content, access requires one of the following: a search warrant, administrative subpoena, grand jury subpoena, or a court order issued under 18 U.S.C. § 2703(d).[56]

As indicated, a warrant is the *only* authorized method for access to the content of ECS records that have been stored 180 days or fewer. In all other cases, a warrant *may* be used, but the SCA also authorizes other forms of legal process — a grand jury subpoena, an administrative subpoena, or a court order issued under Section 2703(d). Those alternatives to a warrant are discussed briefly below.

---

49. See 18 U.S.C. § 2511(2)(g)(i) (it is not unlawful "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public").

50. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th. Cir. 2002) (SCA applied to content of password protected discussion Internet discussion group).

51. 18 U.S.C. § 2510(14) ("'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications ….").

52. 18 U.S.C. § 2711(2) ("remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system ….").

53. See discussion in Memorandum 2014-33, pp. 16-21.

54. See Memorandum 2014-5, pp. 6-7.

55. 18 U.S.C. § 2703(a).

56. *Id.* at (a) & (b).

Grand Jury Subpoena. The Supreme Court has held that the use of a subpoena by a grand jury is permitted under the Fourth Amendment. There is no need for the grand jury to demonstrate probable cause in order to issue a subpoena:

> [T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.[57]

However, a grand jury subpoena must be reasonable. In *Hale v. Henkel*, the Court held that a grand jury subpoena *duces tecum* was unreasonable under the Fourth Amendment because it was "too sweeping in its terms" and violated "the general principle of law with regard to the particularity required in the description of documents necessary to a search warrant or subpoena."[58]

Administrative Subpoena. Many administrative agencies have statutory authority to issue investigative subpoenas.[59] The use of such a subpoena to compel the production of evidence (rather than a warrant) does not violate the Fourth Amendment, so long as the subpoena is authorized, sufficiently definite, and reasonable:

> Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant.[60]

As discussed in a prior memorandum,[61] there is an opinion of the Fourth Circuit that offers a *procedural* justification for the compatibility of an administrative subpoena with the Fourth Amendment. Unlike a warrant, which operates immediately and by surprise, an administrative subpoena provides notice to the person who must produce records, who can then move to quash if the request is unreasonable. That opportunity for judicial review before turning

---

57. United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991).
58. 201 U.S. 43, 76-77 (1906).
59. See Gov't Code §§ 11180-11191.
60. Brovelli v. Superior Court, 56 Cal. 2d 524, 529 (1961) (citing United States v. Morton Salt Co., 338 U.S. 632, 651-654 (1950)); Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.").
61. See Memorandum 2014-33, pp. 23-25.

over any records is sufficient to safeguard against an unreasonable search. An advance judicial determination of probable cause is therefore not required.[62]

One practical difficulty with that rationale is that the SCA does not always require advance notice and an opportunity to quash before an administrative subpoena will operate. A court can defer notice to the target of the subpoena for repeated 90-day periods, so long as there is reason to believe that giving the notice would produce one of the following "adverse results:"

> (A) endangering the life or physical safety of an individual;
> (B) flight from prosecution;
> (C) destruction of or tampering with evidence;
> (D) intimidation of potential witnesses; or
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[63]

This suggests that the procedural rationale for the compatibility of an administrative subpoena with the requirements of the Fourth Amendment may not apply when a subpoena is used without actual prior notice to the person whose records are obtained. That issue is discussed later in this memorandum.[64]

Court Order Under 18 U.S.C. § 2703(d). Finally, as noted above, the SCA allows access to stored communications with a court order issued pursuant to 18 U.S.C. § 2703(d).

Such an order resembles a warrant more than an administrative subpoena. Like a warrant, it can be used by law enforcement to investigate a violation of criminal law (by contrast, an administrative subpoena is generally used by administrative agency officials to investigate a violation of civil regulatory laws). The Section 2703(d) order is approved by a court in advance of its operation (by contrast, an administrative subpoena is subject to judicial review only *after* it has been served). Finally, a Section 2703(d) order is only subject to a motion to quash filed by the service provider who holds the requested records, on the limited grounds of undue burden to the service provider (by contrast, an administrative subpoena can be challenged in court by the person whose records are being requested, on constitutional grounds).

---

62. *In re* Subpoena Duces Tecum, 228 F.3d 341, 347-48 (4th Cir. 2000) (citations omitted). See also *Brovelli*, 56 Cal. 2d at 529 (legally authorized and reasonable administrative subpoena complies with Article I, Section 13 of California Constitution).
63. 18 U.S.C. § 2705(a).
64. See "Administrative Subpoena," *infra* pp. 24-27.

Despite the fact that an order issued under Section 2703(d) is functionally similar to a warrant, probable cause is not required for its issuance. Instead, the order will issue "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

For those reasons, a Section 2703(d) order seems insufficient to satisfy the Fourth Amendment and Article I, Section 13 of the California Constitution.

Recall, however, that there is no reasonable expectation of privacy, for purposes of the Fourth Amendment, in information that is voluntarily provided to a third party. This suggests that the Fourth Amendment may not apply to the use of a Section 2703(d) order to access a person's communication data that is being stored by a third party.[65] That argument has been undermined somewhat by the recent decision in *United States v. Warshak*, in which the court held that the content of email is protected by the Fourth Amendment, notwithstanding the third party doctrine.[66]

More importantly for the purposes of this study, Article I, Section 13 of the California Constitution is not subject to a third party doctrine limitation. In the absence of that limitation, it seems probable that a person has a reasonable expectation of privacy with respect to the content of stored communications, for the purposes of the California Constitution's search and seizure requirements. If that is correct, the use of Section 2703(d) to access such information, without a judicial finding of probable cause, would be a violation of Article I, Section 13.

What Level of Legal Process Should be Required?

It is possible that the Fourth Amendment is inapplicable to the content of any stored electronic communications, because all stored communications have been voluntarily provided to a third party, defeating any reasonable expectation of privacy as to their content. Recent case law developments, like the *Warshak* decision finding the Fourth Amendment applicable to stored email, create some room for doubt about the effect of the third party doctrine as applied to

65. See, e.g., *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional.").

66. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

electronic communications. But the Supreme Court has not yet directly addressed the issue, leaving the existing third party jurisprudence in place.

However, the California Supreme Court has held that there is no third party doctrine limitation on Article I, Section 13 of the California Constitution. The fact that information is voluntarily provided to a third party for a limited purpose does not, by itself, defeat a reasonable expectation of privacy in that information. In the absence of the third party doctrine, there would seem to be a reasonable expectation of privacy, under Article I, Section 13, with regard to the content of stored electronic communication.

In order to protect the constitutional right provided in Article I, Section 13, the proposed law should require a warrant, administrative subpoena, or grand jury subpoena in order to access stored electronic communications. Use of a Section 2703(d) order is probably not compatible with Article I, Section 13 and should therefore not be included in the proposed legislation. Omission of Section 2703(d) should not create any preemption problem. The SCA expressly authorizes states to opt out of Section 2703(d).[67]

However, there is a provision of the SCA that could partially preempt the approach described above. Under that statute, stored communication content that is in ECS storage for 180 days or fewer can *only* be accessed with a warrant.[68] This effectively prohibits access by means of a grand jury subpoena or administrative subpoena. In order to avoid preemption, the proposed legislation should probably preserve that rule.

To summarize, in order to comply with existing constitutional and statutory requirements, the proposed legislation should require the following types of legal process for state or local government access to the content of stored electronic communications:

- For ECS content stored 180 days or fewer, a warrant.
- For all other stored electronic communication content, one of the following: a warrant, administrative subpoena, or grand jury subpoena.

It is important to note that the second rule would not really present a government official with a *choice*. Each of the instruments listed is used in a different context. A warrant can only be used by a "peace officer" who is

67. 18 U.S.C. § 2703(d) ("In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.")
68. 18 U.S.C. § 2703(a).

conducting a criminal investigation.[69] An administrative subpoena can only be used by an administrative agency that is investigating a violation of the laws within its limited regulatory jurisdiction.[70] And a grand jury subpoena can only be used by a grand jury.[71]

Opportunities for Reform

Use of Warrant by Administrative Agency or Grand Jury

As noted above, the SCA requires a warrant in order for government to access the content of ECS information that has been stored for 180 days or fewer. This appears to preclude the use of an administrative or grand jury subpoena to access such information.

That rule may have the indirect effect of *barring* access to such information by an administrative agency or grand jury. That is because, in general, an administrative agency or grand jury cannot lawfully obtain a warrant.

In California, a search warrant is "directed to a peace officer"[72] and its use is generally limited to situations involving a criminal investigation.[73]

In general, a "peace officer" is a city police officer, county sheriff or deputy sheriff, game warden, Department of Justice special agent, or other public official who exercises "police functions."[74] With a few exceptions,[75] an administrative agency's regulatory investigators are not peace officers. Moreover, most regulatory law enforcement is civil in nature, rather than criminal. Thus, an administrative enforcement officer is generally unable to obtain a search warrant.

While it is true that a grand jury can investigate crimes, the staff does not believe that a grand jury could ever be understood to be a "peace officer."

For those reasons, it is not clear that a search warrant can be directed to an administrative agency or grand jury.

In practice, that may not be a problem for a grand jury, because existing law provides that a district attorney can provide assistance to a grand jury.[76] This would seem to provide an indirect way that a grand jury could employ a warrant

69. Penal Code §§ 1523-1524.
70. 18 U.S.C. § 2703(b)(B)(i); Gov't Code §§ 11180-11181.
71. Penal Code § 939.2.
72. Penal Code § 1523.
73. Penal Code § 1524(a).
74. Penal Code § 830.6.
75. See, e.g., Fish & Game Code §§ 851 (deputized DFW employee is "peace officer"), 878 (county game warden is "peace officer").
76. Penal Code §§ 936, 939.1, 939.7.

to obtain records that cannot be obtained by subpoena (by having the district attorney do so).

But the SCA's "warrant only" rule could be a complete bar against an administrative agency accessing the content of ECS information stored for 180 days or fewer. The staff sees no obvious policy rationale for that result. **Should the issue be addressed in the proposed legislation?** If so, one possibility would be to expressly authorize an administrative agency to obtain a search warrant for the limited purpose of obtaining ECS content that has been stored for 180 days or fewer.[77]

Eliminate ECS/RCS Distinction

For the most part, the approach described in this memorandum would not require continuation of the distinction drawn in the SCA between ECS and RCS information. That would be an improvement, as it would reduce the use of an obsolete distinction of questionable value, the precise boundaries of which require reference to federal case law.

Unfortunately, it may be necessary to preserve the distinction for one purpose — continuing the existing SCA rule that requires the use of a warrant when accessing ECS data that has been stored for 180 days or fewer. That special rule depends on the meaning of ECS, which in turn depends in part on the meaning of RCS.

However, it might be possible to completely eliminate reliance on the ECS/RCS distinction if the rule described above were modified slightly. Instead of requiring a warrant for ECS data that is stored for 180 days or fewer, the rule could be broadened to require a warrant for *any* communication content (ECS or RCS) that has been stored for 180 days or fewer.

This should not present a preemption problem, because such a rule would be at least as protective of privacy as the existing rule (i.e., government access to ECS data stored for 180 days or fewer would still require a warrant).

The downside of this approach is that it would eliminate the option of using an administrative subpoena in some cases where a subpoena can currently be used — to access RCS data that has been stored for 180 days or fewer. That additional constraint on administrative agency investigations could be ameliorated somewhat if the reform possibility discussed immediately above

77. For an apparent example of a similar provision, see Code Civ. Proc. §§ 1822.50-1822.60 (authorizing administrative "inspection warrants").

were implemented (i.e., if an administrative agency could instead obtain a warrant to access such information). **Should this possibility be explored further?**

Administrative Subpoena

As discussed above, courts have held that a reasonable administrative subpoena can be used to access records without violating the Fourth Amendment or Article I, Section 13 of the California Constitution.

In explaining why an administrative subpoena is sufficient to satisfy constitutional search and seizure requirements, one court emphasized the fact that a subpoena involves notice and an opportunity to quash before producing any records. As discussed above, that procedural rationale depends on advance notice actually being given to the target of the subpoena. But under the SCA, notice can be delayed by court order, so that the records are produced before the target has notice. In a prior memorandum, the staff wondered whether that could be a problem under Article 1, Section 13 of the California Constitution.[78]

Since raising that issue, the staff has found new information that seems to support the constitutionality of using an administrative subpoena to obtain customer records, even if advance notice is not given to the customer:

(1) The special nature of administrative investigations may diminish the reasonable expectation of privacy with regard to information sought by administrative subpoena.
(2) California law expressly permits the use of administrative subpoenas, without advance notice to a customer, to obtain financial records that are protected by Article 1, Section 13 of the California constitution.

Those two points are discussed further below.

Special Nature of Administrative Investigations. An administrative agency is charged with enforcing a specific set of regulatory laws that are within its statutory jurisdiction. The courts have found good reason to treat a search conducted as part of an administrative investigation differently than a search conducted in a general criminal investigation.

First, many of the records that an administrative agency might seize in connection with an investigation are records that the law requires to be kept, for

78. See Memorandum 2014-33, p. 25.

regulatory purposes. The expectation of privacy with respect to such records is reduced:

> [N]o Fourth Amendment "privacy" claim can be asserted against an administrative [subpoena] limited to the production of records which the [subpoenaed] party is required to maintain, for the express purpose of agency inspection, under lawful statutes or regulations.[79]

More generally, those who participate in regulated activities may expect greater administrative intrusion into their privacy, as a consequence of the choice to take part in the regulated activity. "As regulatory schemes have become increasingly important in enforcing laws designed to protect the public's health and welfare, reliance on 'probable cause' as a means of restraining agency [subpoena] power has all but disappeared."[80]

This does not mean that constitutional search and seizure requirements are *inapplicable* to an administrative investigation. Instead, courts have held that the constitutional requirements for use of an administrative subpoena are *different* from those governing the use of a warrant:

> Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant.[81]

Use of Administrative Subpoenas Under Existing California Law. The California Right to Financial Privacy Act ("CRFPA") generally prohibits state or local government access to customer records held by financial institutions in California.[82]

In addition to an exception for access pursuant to a search warrant,[83] the CFRPA has an exception for records requested pursuant to an administrative subpoena.[84] That exception is expressly conditioned on notice being given to the

79. Craib v. Bulmash, 49 Cal. 3d 475, 483 (1989).
80. *Id.* at 481.
81. Brovelli v. Superior Court, 56 Cal. 2d 524, 529 (1961) (citing United States v. Morton Salt Co., 338 U.S. 632, 651-654 (1950)); Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.").
82. Gov't Code § 7471(a).
83. Gov't Code § 7475.
84. Gov't Code § 7474.

customer whose records are being requested, at least 10 days before the records are produced. The customer has standing to move to quash the subpoena.[85]

However, the CRFPA allows a court to waive or shorten the required notice. To do so, the court must find "a reasonable inference that a law subject to the jurisdiction of the petitioning agency has been or is about to be violated…."[86] The delayed notice must be given within 60 days after the search (subject to an unlimited number of 30 day extensions for "good cause").

Thus, the CRFPA expressly allows the use of an administrative subpoena to access customer financial records in circumstances in which there is no advance notice to the customer and no opportunity to quash.

That has been the rule since the CRFPA was first enacted in 1976, just two years after the California Supreme Court's decision in *Burrows v. Superior Court*, which held that a person has a reasonable expectation of privacy, for the purposes of Article I, Section 13 of the California Constitution, in financial records held by a financial institution.[87] This timing strongly suggests that the CRFPA was enacted as a reaction to *Burrows*, to establish clear procedures to implement the Court's holding. That suggestion is reinforced by an express statement of the Legislature's purpose:

> The Legislature finds and declares as follows:
> (a) Procedures and policies governing the relationship between financial institutions and government agencies have in some cases developed without due regard to citizens' constitutional rights.
> (b) The confidential relationships between financial institutions and their customers are built on trust and must be preserved and protected.
> (c) The purpose of this chapter is to clarify and protect the confidential relationship between financial institutions and their customers and to balance a citizen's right of privacy with the governmental interest in obtaining information for specific purposes and by specified procedures as set forth in this chapter.[88]

Given the Legislature's express intention that the CRFPA protect customers' constitutional rights, at a time when the Court's expression of those rights was fresh in everyone's minds, it would be surprising if the CRFPA's administrative subpoena rule were unconstitutional. Moreover, the staff did not find any published court opinion in which the constitutionality of the administrative

85. *Id.* at (a).
86. *Id.* at (b).
87. Burrows v. Superior Court, 13 Cal. 3d 238 (1974).
88. Gov't Code § 7461.

subpoena provision was challenged. Proposition 8 does not fully explain the lack of such a challenge, as the Truth-in-Evidence rule barring the exclusion of relevant evidence in criminal cases was not added to the California Constitution until six years after the enactment of the CRFPA.

Conclusion. It is not clear that prior notice of the use of an administrative subpoena to obtain stored electronic communication content is constitutionally necessary. There are cases holding that the use of a reasonable administrative subpoena is compatible with the Fourth Amendment, without any mention of prior notice being required. Moreover, the California Legislature and Governor enacted a statute that authorizes the use of an administrative subpoena without prior notice, to access records that were known to be protected by Article I, Section 13 of the California Constitution, in a bill that was expressly stated to be about preserving constitutional privacy rights.

For those reasons, the staff recommends that administrative subpoenas be treated the same way that they are in the SCA. Notice to the customer should generally be required, but be subject to waiver by a court in specified exigent circumstances. In other words, existing law on the issue would be continued.

Privileged Content in Stored Communications

Penal Code Section 1524(c) provides a special procedure for the issuance of a warrant that is used to obtain records that are "in the possession or under the control of" an attorney, doctor, psychotherapist, or clergy member (unless such a person is reasonably suspected of engaging in a crime related to the requested records).

When issuing the warrant, the court must appoint a special master to accompany law enforcement when the warrant is served. If requested records are not produced, the special master will conduct any search that may be necessary to find the records. If the holder of a requested record asserts that the record should not be disclosed, the special master will seal that record and present it to the court for a hearing on the issue.[89] The effect is to shield potentially privileged material from disclosure to law enforcement.

It is not clear whether or how this procedure would apply when a warrant is issued to seize the content of electronic communications stored by a communication service provider. For example, suppose that law enforcement

89. Penal Code § 1524(c)-(d).

obtains a warrant to obtain the stored email of a person who is known to be an attorney. Are such records in the attorney's "possession" or under the attorney's "control," so as to trigger the application of the special master requirement of Section 1524(c)? The staff has not found any published case addressing such issues. **Should the matter be addressed as part of this study?**

METADATA

The preceding part of the memorandum discussed the *content* of stored communications.

This part discusses *non-content* information about electronic communications (also known as "metadata," or information about information). A classic example of metadata is the numbers dialed on a telephone. But it could also include the date, time, duration, or size of a communication; the name and address of a subscriber who communicates anonymously or using a pseudonym; the address of locations visited on the Internet; the terms used in conducting Internet searches; and location data that is collected as an incident of using a mobile communication device.

The tracking of location data raises unique constitutional and statutory issues. It will be discussed separately, in a supplement to this memorandum.

Constitutional and Statutory Requirements

Fourth Amendment

In *Smith v. Maryland*,[90] the Court found no subjective or objectively reasonable expectation of privacy in the numbers dialed on a telephone, because that information is voluntarily provided to a third party.

Although there is no United States Supreme Court decision directly on point, federal circuit courts have applied the same principle to Internet metadata. For example, in *United States v. Forrester*,[91] police requested that an ISP install a "mirror port" to track information about the defendant's Internet usage. The mirror port "enabled the government to learn the to/from addresses of [defendant's] e-mail messages, the IP addresses of the websites that [defendant] visited and the total volume of information sent to or from his account."[92] After reiterating the holding of *Smith*, that the use of a pen register to collect telephone

90. 442 U.S. 735 (1979).
91. 512 F. 3d 500 (9th Cir. 2008).
92. *Id*. at 505.

dialing information is not a Fourth Amendment search, the Ninth Circuit held that the government's use of the mirror port was "constitutionally indistinguishable from the use of a pen register."[93] Thus, there does not appear to be a reasonable expectation of privacy, for the purposes of the Fourth Amendment, in electronic communication metadata.

Article I, Section 13 of the California Constitution

As noted above, the California Supreme Court has not adopted the third party doctrine with regard to Article I, Section 13 of the California Constitution, even with respect to pure metadata.

In *Burrows v. Superior Court*,[94] the Court held that a person has a reasonable expectation of privacy, for the purposes of Article I, Section 13 of the California Constitution, in the person's bank records. The Court cited two main reasons for its conclusion: (1) The disclosure of such information to third parties is an unavoidable part of modern life. (2) Access to such information can reveal a "virtual current biography" of a person.[95] In *California v. Blair*,[96] the California Supreme Court extended the reasoning of *Burrows* to records of credit card use and the numbers dialed on a telephone.

The reasoning described above seems to apply with equal force to metadata relating to electronic communications. If a list of telephone numbers dialed can provide a virtual current biography, then that must also be true for a list of email correspondents or a website browsing history. For example, the United States Supreme Court recently discussed the importance of the privacy of such metadata (in the context of a custodial search of a cell phone):

> An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.[97]

In short, if Article I, Section 13 of the California Constitution protects the privacy of telephone numbers dialed, it almost certainly protects the privacy of electronic communication metadata. Use of modern electronic communications is as unavoidable as use of the telephone was in 1979. Detailed historical

93. *Id*. at 510-11 (footnotes omitted).
94. 13 Cal. 3d 238 (1974).
95. *Id*. at 247-48.
96. 25 Cal. 3d 640 (1979).
97. Riley v. California, 134 S. Ct. 2473, 2489 (2014).

information about the use of such communications probably provides more of a "virtual current biography" than the numbers dialed on a telephone.

Freedom of Expression

Government access to electronic communication metadata could have the same types of chilling effects on free expression as government access to communication content. The analysis set out earlier applies here as well.[98]

Stored Communication Act

The federal Stored Communication Act provides special rules for government access to non-content information about customer communications.[99] Those rules are equally applicable to both ECS and RCS information.

In general, stored electronic communication metadata can be obtained by government through the use of a warrant or a court order issued under 18 U.S.C. § 2703(d).[100] Importantly, such information cannot be accessed using a grand jury subpoena or administrative subpoena. That is counter-intuitive, because there are circumstances in which a grand jury or administrative subpoena can be used to access the *content* of communications.[101] The staff sees no obvious policy reason for this odd treatment of subpoenas.

There is also a special rule for access to the following types of customer account information:

> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;
> (D) length of service (including start date) and types of service utilized;
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> (F) means and source of payment for such service (including any credit card or bank account number)

With regard to that subset of customer account information, government access can be authorized by a warrant, grand jury subpoena, administrative subpoena, or Section 2703(d) order.[102]

98. See supra pp. 14-16.
99. 18 U.S.C. § 2703(c).
100. There is also a special rule relating to telemarketing fraud. *Id.* at (c)(1)(D).
101. *Id.* at (b).
102. *Id.* at (c)(2).

Pen Register and Trap and Trace Device

While the SCA governs access to *historical* information about telephone numbers dialed or received by a customer,[103] access to such information about *future* calls is governed by the federal Pen Register and Trap and Trace Device statute.[104]

A special court order is required to authorize use of a pen register or trap and trace device. The substantive standard for issuance of such an order is fairly low. The law enforcement officer requesting the order need only certify that the information sought is relevant to an ongoing criminal investigation.[105]

Noncontent Evidence of Specified Misdemeanors

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

> showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery.[106]

Legislative history indicates that this provision was added to combat identity theft, which can involve a large number of relatively modest property crimes.[107]

What Level of Legal Process Should be Required?

It is clear that Article I, Section 13 of the California Constitution applies to noncontent metadata such as dialed telephone numbers. Given that, it is almost certain that Section 13 applies to noncontent electronic communication metadata. Therefore, in order to preserve existing constitutional rights, the proposed legislation should be consistent with constitutional search and seizure requirements (i.e., a warrant, administrative subpoena, or grand jury subpoena should be required for state or local agency access to electronic communication metadata).

103. 18 U.S.C. § 2703(c)(2)(C).
104. 18 U.S.C. § 3121 *et seq*.
105. 18 U.S.C. § 1323(a).
106. Penal Code § 1524(a)(7).
107. Senate Public Safety Committee Analysis of SB 1980 (April 30, 2002), pp. 4-5.

While the SCA would allow access to metadata with a court order issued under 18 U.S.C. § 2703(d), such an order does not appear to be sufficient to satisfy the requirements of Article I, Section 13 of the California Constitution. For that reason, use of a Section 2703(d) order to authorize access to metadata should not be included in the proposed legislation. As noted before, this would not present a preemption problem, because the SCA expressly permits states to opt out of Section 2703(d).

However, it is important to recognize the likelihood of federal preemption with regard to the use of a *subpoena* in certain situations. As discussed above, the SCA only provides for the use of a *warrant* when government seeks access to general electronic communication metadata (as distinguished from a specified subset of customer information — name, address, telephone connection records, length of service, subscriber number or other identity, means of payment — which can be obtained with a subpoena).[108] Similarly, access to information about a person's audiovisual viewing history can only be obtained with a warrant.[109]

As only a warrant can be used in those two situations, there is an argument that California law would be preempted if it were to permit the use of a subpoena. For that reason, the proposed law should probably not permit the use of a subpoena to access general electronic communication metadata or audiovisual viewing history.

To summarize, in order to protect established constitutional rights and avoid federal preemption, **the proposed legislation should require the following forms of authorization for state or local government agency access to noncontent electronic communication metadata:**

- In general, a warrant.
- For customer account information, a warrant, administrative subpoena, or grand jury subpoena.

Opportunities for Reform

Use of Warrant by Administrative Agency or Grand Jury

As noted above, the SCA does not authorize the use of a subpoena to access electronic communication metadata.

108. *Id.* at (c)(2).
109. 18 U.S.C. § 2710.

That rule could have the indirect effect of *barring* access to such information by an administrative agency or grand jury. That is because, as discussed earlier, an administrative agency or grand jury generally cannot obtain a warrant.

Thus, the SCA's "warrant only" rule could be a complete bar against an administrative agency accessing metadata (even though they can access some *content* with an administrative subpoena). The staff sees no obvious policy rationale for that result. **Should the issue be addressed in the proposed legislation?** If so, one possibility would be to expressly authorize an administrative agency to obtain a search warrant for the limited purpose of accessing electronic communication metadata.

CONCLUSION

The Commission needs to decide what level of legal process should be required for state and local agency access to each of the distinct categories of electronic communication information.

This memorandum describes, for each of the categories, the apparent constitutional and statutory minimums that must be respected in the proposed legislation. To summarize:

Type of Access	**Minimum Required Process**
Prospective Interception	Super-Warrant
ECS Content Stored 180 days or Fewer	Warrant
All Other Stored Content	Warrant, Administrative Subpoena, or Grand Jury Subpoena
General Metadata	Warrant
Customer Account Metadata	Warrant, Administrative Subpoena, or Grand Jury Subpoena

The memorandum does not specifically discuss the numerous important ancillary matters that will need to be included in the proposed legislation, which include:

- The general prohibitions on access to protected information.
- The various exceptions to those general prohibitions.
- Remedies for violation of the general prohibitions.
- The procedures used by government to obtain authorization for access to information.

- Safe harbors for communication service providers who rely in good faith on lawful process.

Unless the Commission wishes to take a different approach, the staff will draft the proposed legislation so as to preserve existing statutory law on such matters (with a priority on preserving California law where it differs from, but would not be preempted by, federal law). If any problem or opportunity for reform becomes apparent in the course of the drafting process, the staff will present it to the Commission for a decision on how best to resolve it.

In addition, the proposed legislation could address any of the possible reforms noted in this memorandum. To summarize:

Type of Access	**Possible Reforms**
Prospective Interception	• Define "interception" to mean prospective access. • Minimize interception of privileged material in non-streaming content. • Modernize identification of the "facility" to be tapped.
Stored Content	• Authorize administrative agency use of a warrant to obtain content that requires a warrant. • Completely eliminate ECS/RCS distinction. • Clarify whether or how "special master" procedures for access to privileged material apply to stored electronic content.
Metadata	• Authorize administrative agency use of a warrant to obtain metadata that requires a warrant.

Once the Commission has made decisions on the issues discussed above, the staff will begin drafting implementing legislation.

Respectfully submitted,

Brian Hebert
Executive Director