

CALIFORNIA LAW REVISION COMMISSION

TENTATIVE REPORT

State and Local Agency Access to Electronic Communications: Constitutional and Statutory Requirements

April 2015

The purpose of this tentative report is to solicit public comment on the Commission's tentative conclusions. A comment submitted to the Commission will be part of the public record. The Commission will consider the comment at a public meeting when the Commission determines what, if any, report it will make to the Legislature. It is just as important to advise the Commission that you approve the tentative report as it is to advise the Commission that you believe revisions should be made to it.

COMMENTS ON THIS TENTATIVE REPORT SHOULD BE RECEIVED BY THE COMMISSION NOT LATER THAN June 15, 2015.

The Commission will often substantially revise a proposal in response to comment it receives. Thus, this tentative report is not necessarily the report the Commission will submit to the Legislature.

California Law Revision Commission
4000 Middlefield Road, Room D-2
Palo Alto, CA 94303-4739
650-494-1335
<commission@clrc.ca.gov>

SUMMARY OF TENTATIVE REPORT

The California Law Revision Commission has been directed to prepare proposed legislation on state and local agency access to customer records of communication service providers. In doing so, the Commission was expressly directed to protect customers' existing constitutional rights.

As a first step in complying with that mandate, the Commission researched the relevant constitutional and statutory requirements for government access to electronic communications and related records. This tentative report summarizes the Commission's findings regarding controlling federal and state constitutional rights and federal statutory law. A 2-page explanation of the Commission's tentative conclusions appears at the end of the report.

This report was prepared pursuant to Resolution Chapter 115 of the Statutes of 2013.

CONTENTS

SCOPE OF REPORT	1
CONSTITUTIONAL LAW	2
Search and Seizure	2
Fourth Amendment of the United States Constitution	2
Third Parties and the Fourth Amendment	6
Third Parties and Article I, Section 13 of the California Constitution	11
Additional Considerations in Special Cases	14
Interception of Communications	14
Location Tracking	16
Investigative Subpoena	17
Summary of Search and Seizure Requirements	20
Freedom of Expression	21
Associational Privacy	22
Anonymous Speech	24
Reader Privacy	26
Private Speech	28
Press Confidentiality	29
Conclusion	30
Privacy	30
“Penumbral” Privacy Right in the United States Constitution	30
Autonomy Privacy	32
Informational Privacy	33
Informational Privacy and the Fourth Amendment	36
Summary of Federal Constitutional Privacy Right	36
Express Privacy Right in the California Constitution	37
Private Action	40
Elements of the Privacy Right	40
Standard of Review	44
Informational Privacy and Article I, Section 13 of the California Constitution	46
Summary of California Constitutional Privacy Right	47
FEDERAL SURVEILLANCE STATUTES	48
Interception of Communication Content	49
Access to Stored Communications	55
Video Privacy Protection Act	63
Pen Register Act	64
Location Tracking	67
OTHER FEDERAL PRIVACY STATUTES	69
Health Insurance Portability and Accountability Act of 1996	69
Cable Communication Policy Act of 1984	71
Privacy Protection Act of 1980	72
Family Education Rights and Privacy Act of 1974	73
BRIEF LIST OF CALIFORNIA PRIVACY STATUTES	73
SUMMARY OF FINDINGS	75

STATE AND LOCAL AGENCY ACCESS TO ELECTRONIC COMMUNICATIONS

SCOPE OF REPORT

1
2 The Commission has been directed to prepare comprehensive legislation on state
3 and local agency access to customer information that the agency obtains from a
4 communication service provider.¹

5 The purpose of the proposed legislation is to clarify and modernize the law,
6 while preserving existing constitutional rights, enabling law enforcement to
7 protect public safety, and providing clear procedures to be followed when
8 government requests access to information held by communication service
9 providers.²

10 As a first step in this study, the Commission examined the existing
11 constitutional law on the matter. Both the United States and California
12 Constitutions were examined. This report describes the Commission's findings
13 regarding constitutional limitations on government access to electronic
14 communications.

15 The Commission also examined relevant federal and state statutory law. Federal
16 law that is binding on the states is also described in this report. The report does not
17 comprehensively discuss relevant California statutory law, because the Legislature
18 can revise such law (with the Governor's approval or acquiescence).

19 The scope of this report is bounded by the extent of the authority conferred by
20 the Legislature. The Commission is authorized to study *state and local*
21 *government* access to electronic communication information that is *obtained from*
22 *communication service providers*. Pursuant to that limited mandate, this report
23 does not address any of the following matters:

- 24 • Information obtained by the federal government.
- 25 • Information obtained by private persons.
- 26 • Information obtained directly from a communication customer, rather than
27 from that person's service provider (e.g., by means of eavesdropping,
28 searching a person's computer or cell phone, or directly intercepting radio
29 transmissions).

30 In addition, this report does not address access to information through discovery
31 in a civil, criminal, or administrative adjudicative proceeding. Such access is
32 supervised by the court, which can hear and address any constitutional or statutory
33 objections to the disclosure of information. For that reason, discovery does not

1. 2013 Cal. Stat. res. ch. 115 (SCR 54 (Padilla)).

2. *Id.*

1 present the same issues as surveillance conducted as part of a pre-trial
2 investigation.

3 CONSTITUTIONAL LAW

4 There are a number of constitutional rights that could be affected by government
5 access to information about a person's electronic communications.

6 The most obvious is the constitutional protection against unreasonable search
7 and seizure, afforded by the Fourth Amendment of the United States Constitution
8 and Article I, Section 13 of the California Constitution.

9 Electronic communication surveillance could also unconstitutionally interfere
10 with the rights of privacy and free expression.

11 Those constitutional rights are discussed below.

12 Search and Seizure

13 **Fourth Amendment of the United States Constitution**

14 The Fourth Amendment of the United States Constitution provides:

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

20 When the Fourth Amendment was ratified, electronic communications did not
21 exist. Searches and seizures were material and involved some kind of trespass
22 against a person or that person's property.

23 With the advent of telephones and electronic microphones, it became possible to
24 listen in on private conversations remotely, without any physical touching of the
25 person or property of the subject of the surveillance. This presented a novel
26 question: Does the Fourth Amendment protect the general privacy of
27 communications against government intrusion? Or does it only protect the security
28 of one's person and property?

29 The Supreme Court answered that question in *Olmstead v. United States*,³ the
30 first wiretapping case decided by the Court. In *Olmstead*, federal prohibition
31 agents tapped the office and home telephones of persons they suspected of
32 illegally importing and distributing liquor. In establishing the wiretaps, the federal
33 agents did not enter the suspects' property. Instead, they tapped wires in the
34 basement of an office building and on roadside telephone poles. Because there had
35 been no physical intrusion on a suspect's person or property, the Court held that
36 there was no "search" within the meaning of the Fourth Amendment:

3. 277 U.S. 438 (1928).

1 The amendment itself shows that the search is to be of material things — the
2 person, the house, his papers, or his effects. The description of the warrant
3 necessary to make the proceeding lawful is that it must specify the place to be
4 searched and the person or *things* to be seized.

5 ...

6 The amendment does not forbid what was done here. There was no searching.
7 There was no seizure. The evidence was secured by the use of the sense of
8 hearing, and that only. There was no entry of the houses or offices of the
9 defendants.

10 By the invention of the telephone fifty years ago and its application for the
11 purpose of extending communications, one can talk with another at a far distant
12 place. The language of the Amendment cannot be extended and expanded to
13 include telephone wires reaching to the whole world from the defendant’s house
14 or office. The intervening wires are not part of his house or office any more than
15 are the highways along which they are stretched.

16 ...

17 Congress may, of course, protect the secrecy of telephone messages by making
18 them, when intercepted, inadmissible in evidence in federal criminal trials by
19 direct legislation, and thus depart from the common law of evidence. But the
20 courts may not adopt such a policy by attributing an enlarged and unusual
21 meaning to the Fourth Amendment. The reasonable view is that one who installs
22 in his house a telephone instrument with connecting wires intends to project his
23 voice to those quite outside, and that the wires beyond his house and messages
24 while passing over them are not within the protection of the Fourth Amendment.
25 Here, those who intercepted the projected voices were not in the house of either
26 party to the conversation.⁴

27 Justice William Brandeis wrote a prescient dissent, which is worth quoting at
28 some length:

29 “Legislation, both statutory and constitutional, is enacted, it is true, from an
30 experience of evils, but its general language should not, therefore, be necessarily
31 confined to the form that evil had theretofore taken. Time works changes, brings
32 into existence new conditions and purposes. Therefore, a principle, to be vital,
33 must be capable of wider application than the mischief which gave it birth. This is
34 peculiarly true of constitutions. They are not ephemeral enactments, designed to
35 meet passing occasions. They are, to use the words of Chief Justice Marshall
36 ‘designed to approach immortality as nearly as human institutions can approach
37 it.’ The future is their care, and provision for events of good and bad tendencies of
38 which no prophecy can be made. In the application of a constitution, therefore,
39 our contemplation cannot be only of what has been, but of what may be. Under
40 any other rule, a constitution would indeed be as easy of application as it would
41 be deficient in efficacy and power. Its general principles would have little value,
42 and be converted by precedent into impotent and lifeless formulas. Rights
43 declared in words might be lost in reality.”

44 When the Fourth and Fifth Amendments were adopted, “the form that evil had
45 theretofore taken” had been necessarily simple. Force and violence were then the

4. *Id.* at 464-65 (emphasis in original).

1 only means known to man by which a Government could directly effect self-
2 incrimination. It could compel the individual to testify — a compulsion effected,
3 if need be, by torture. It could secure possession of his papers and other articles
4 incident to his private life — a seizure effected, if need be, by breaking and entry.
5 Protection against such invasion of “the sanctities of a man’s home and the
6 privacies of life” was provided in the Fourth and Fifth Amendments by specific
7 language. ... But “time works changes, brings into existence new conditions and
8 purposes.” Subtler and more far-reaching means of invading privacy have become
9 available to the Government. Discovery and invention have made it possible for
10 the Government, by means far more effective than stretching upon the rack, to
11 obtain disclosure in court of what is whispered in the closet.

12 Moreover, “in the application of a constitution, our contemplation cannot be
13 only of what has been but of what may be.” The progress of science in furnishing
14 the Government with means of espionage is not likely to stop with
15 wiretapping....⁵

16 The narrow trespass-based approach taken to wiretapping in *Olmstead* prevailed
17 until 1967, when the Supreme Court decided *Katz v. United States*.⁶

18 *Reasonable Expectation of Privacy*

19 Strictly speaking, *Katz* was not a wiretap case. In *Katz*, FBI agents had placed a
20 listening device on the outside of a public telephone booth. They used it to listen
21 to one end of the telephone calls made by the defendant. There was no direct
22 electronic interception of the calls as they passed through the telephone company’s
23 network.

24 Because the calls were placed in a public telephone booth, and the listening
25 device was positioned on the outside of the telephone booth, there was no trespass
26 against the defendant’s person or property. Under the reasoning adopted in
27 *Olmstead*, it seems clear that the Fourth Amendment would be inapplicable. (In
28 fact, the Supreme Court had applied the same reasoning to a non-wiretap case in
29 *Goldman v. United States*,⁷ which involved the use of a listening device pressed
30 against a wall to eavesdrop on conversations in the next room. Because the device
31 did not involve any trespass there was no search within the meaning of the Fourth
32 Amendment.)

33 In *Katz*, the court abandoned the narrow trespass-based view of eavesdropping:

34 We conclude that the underpinnings of *Olmstead* and *Goldman* have been so
35 eroded by our subsequent decisions that the “trespass” doctrine there enunciated
36 can no longer be regarded as controlling. The Government’s activities in
37 electronically listening to and recording the petitioner’s words violated the
38 privacy upon which he justifiably relied while using the telephone booth, and thus

5. *Id.* at 473-75 (Brandeis, J., dissenting), quoting *Weems v. United States*, 217 U.S. 349 (1910) (citations omitted).

6. 389 U.S. 347 (1967).

7. 316 U.S. 129 (1942).

1 constituted a “search and seizure” within the meaning of the Fourth Amendment.
2 The fact that the electronic device employed to achieve that end did not happen to
3 penetrate the wall of the booth can have no constitutional significance.⁸

4 In a concurring opinion, Justice Harlan set out the now-familiar standard for
5 determining the application of the Fourth Amendment — whether one has a
6 “reasonable expectation of privacy.”

7 As the Court’s opinion states, “the Fourth Amendment protects people, not
8 places.” The question, however, is what protection it affords to those people.
9 Generally, as here, the answer to that question requires reference to a “place.” My
10 understanding of the rule that has emerged from prior decisions is that there is a
11 twofold requirement, first that a person have exhibited an actual (subjective)
12 expectation of privacy and, second, that the expectation be one that society is
13 prepared to recognize as “reasonable.” Thus, a man’s home is, for most purposes,
14 a place where he expects privacy, but objects, activities, or statements that he
15 exposes to the “plain view” of outsiders are not “protected,” because no intention
16 to keep them to himself has been exhibited. On the other hand, conversations in
17 the open would not be protected against being overheard, for the expectation of
18 privacy under the circumstances would be unreasonable. . . .

19 The critical fact in this case is that “[o]ne who occupies it, [a telephone booth]
20 shuts the door behind him, and pays the toll that permits him to place a call is
21 surely entitled to assume” that his conversation is not being intercepted. . . . The
22 point is not that the booth is “accessible to the public” at other times. . . , but that it
23 is a temporarily private place whose momentary occupants’ expectations of
24 freedom from intrusion are recognized as reasonable. . . .⁹

25 As indicated, a “reasonable expectation of privacy” is two-pronged: It requires (1)
26 a subjective expectation of privacy that (2) society considers to be objectively
27 reasonable.¹⁰

28 It is now well-established that the Fourth Amendment applies to private
29 conversations, including those that are conducted electronically. However, the
30 Fourth Amendment does not protect conversations that are conducted in such a
31 way as to defeat any reasonable expectation of privacy. As discussed below, an
32 important example of this involves information that is voluntarily disclosed to a
33 third party.

8. *Katz*, 389 U.S. at 353.

9. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

10. See also *Burrows v. Super. Ct.*, 13 Cal. 3d 238 (1974) (applying reasonable expectation of privacy test to Cal. Const. art. I, § 13). The reasonable expectation of privacy standard supplements the historical trespass-based standard; it does not displace the historical standard. Consequently, the Fourth Amendment may apply to a search that involves either a trespass against a person or their property or a violation of a reasonable expectation of privacy. *United States v. Jones*, 132 S. Ct. 945, 952 (2012).

1 **Third Parties and the Fourth Amendment**

2 The Supreme Court has held that there is no reasonable expectation of privacy
3 with regard to information that is voluntarily disclosed to a third party.
4 Consequently, government access to such information is not a search for the
5 purposes of the Fourth Amendment. This “third party doctrine” is important in
6 evaluating the Fourth Amendment’s application to modern electronic
7 communications (e.g., electronic mail, text messages, social media postings), most
8 of which involve the voluntary disclosure of information to a third party (the
9 communication service provider).

10 The third party doctrine developed out of two cases decided in the 1970s, *United*
11 *States v. Miller*¹¹ and *Smith v. Maryland*.¹²

12 *United States v. Miller*

13 In *United States v. Miller*, federal agents used subpoenas prepared by the United
14 States Attorney’s office to require bank officials to produce a suspect’s bank
15 records. The Supreme Court held that this was not an “intrusion into any area in
16 which respondent had a protected Fourth Amendment interest...”¹³

17 In reaching that conclusion, the Court first rejected the argument, grounded in
18 *Boyd v. United States*,¹⁴ that the Fourth Amendment protects against “compulsory
19 production of a man’s private papers.”¹⁵

20 Unlike the claimant in *Boyd*, respondent can assert neither ownership nor
21 possession. Instead, these are the business records of the banks.¹⁶

22 The Court then considered whether defendant had a reasonable expectation of
23 privacy with regard to his bank records. The Court quoted *Katz* for the proposition
24 that “[w]hat a person knowingly exposes to the public ... is not a subject of Fourth
25 Amendment protection.”¹⁷ It then held that defendant had no “legitimate
26 expectation of privacy” in his bank records, which contained only “information
27 voluntarily conveyed to the banks and exposed to their employees in the ordinary
28 course of business.”¹⁸

29 The depositor takes the risk, in revealing his affairs to another, that the
30 information will be conveyed by that person to the Government. ... This Court
31 has held repeatedly that the Fourth Amendment does not prohibit the obtaining of

11. 425 U.S. 435 (1976).

12. 442 U.S. 735 (1979).

13. *Miller*, 425 U.S. at 440.

14. 116 U.S. 622 (1886).

15. *Id.* at 440.

16. *Id.*

17. *Id.* at 442.

18. *Id.*

1 information revealed to a third party and conveyed by him to Government
2 authorities, even if the information is revealed on the assumption that it will be
3 used only for a limited purpose and the confidence placed in the third party will
4 not be betrayed.

5 *Smith v. Maryland*

6 In *Smith v. Maryland*, the police, acting without a warrant, attached a pen
7 register to defendant’s telephone line (a pen register is a device that records all
8 numbers dialed by a telephone).

9 The Court held that this was not a search within the ambit of the Fourth
10 Amendment, because defendant had no reasonable expectation of privacy as to the
11 numbers that he dialed:

12 First, we doubt that people in general entertain any actual expectation of
13 privacy in the numbers they dial. All telephone users realize that they must
14 “convey” phone numbers to the telephone company, since it is through telephone
15 company switching equipment that their calls are completed. All subscribers
16 realize, moreover, that the phone company has facilities for making permanent
17 records of the numbers they dial, for they see a list of their long-distance (toll)
18 calls on their monthly bills. ... Telephone users, in sum, typically know that they
19 must convey numerical information to the phone company; that the phone
20 company has facilities for recording this information; and that the phone company
21 does in fact record this information for a variety of legitimate business purposes.
22 Although subjective expectations cannot be scientifically gauged, it is too much to
23 believe that telephone subscribers, under these circumstances, harbor any general
24 expectation that the numbers they dial will remain secret.¹⁹

25 ...

26 [The analysis in *Miller*] dictates that petitioner can claim no legitimate
27 expectation of privacy here. When he used his phone, petitioner voluntarily
28 conveyed numerical information to the telephone company and “exposed” that
29 information to its equipment in the ordinary course of business. In so doing,
30 petitioner assumed the risk that the company would reveal to police the numbers
31 he dialed. The switching equipment that processed those numbers is merely the
32 modern counterpart of the operator who, in an earlier day, personally completed
33 calls for the subscriber. Petitioner concedes that if he had placed his calls through
34 an operator, he could claim no legitimate expectation of privacy. ... We are not
35 inclined to hold that a different constitutional result is required because the
36 telephone company has decided to automate.²⁰

37 Because the Court found no “reasonable expectation of privacy” with regard to
38 the telephone numbers dialed, government access to such information was not a
39 search within the meaning of the Fourth Amendment.

19. *Smith*, 442 U.S. at 742-43.

20. *Id.* at 744-45 (citations omitted).

1 ***Communication Content v. Metadata***

2 There is some support for the proposition that the third party doctrine does not
3 apply to the content of communications — it only applies to non-content
4 information *about* communications (hereafter “metadata”). Under this theory, the
5 Fourth Amendment protects the content of an email message, but not the address
6 to which the email was delivered (which can be analogized to a telephone number
7 dialed or the address on the outside of a mailed envelope).²¹

8 The Supreme Court noted the distinction between content and metadata in
9 explaining why the use of a pen register is not a Fourth Amendment search:

10 [A] pen register differs significantly from the listening device employed in
11 *Katz*, for pen registers do not acquire the *contents* of communications. This Court
12 recently noted:

13 “Indeed, a law enforcement official could not even determine from the use of a
14 pen register whether a communication existed. These devices do not hear sound.
15 They disclose only the telephone numbers that have been dialed — a means of
16 establishing communication. Neither the purport of any communication between
17 the caller and the recipient of the call, their identities, nor whether the call was
18 even completed is disclosed by pen registers.” *United States v. New York Tel. Co.*,
19 434 U. S. 159, 167 (1977).

20 But the Court did not expressly condition its holding on the content-metadata
21 distinction. Instead, the Court analyzed whether a person has a reasonable
22 expectation of privacy with regard to information that is voluntarily disclosed to a
23 third party (a question which could be asked as readily about content as about
24 metadata).

25 Another obstacle to the theory discussed above is that one of the seminal third
26 party doctrine cases did not involve metadata. In *Miller*, the government accessed
27 the *content* of a person’s bank records. The theory could perhaps be salvaged by
28 drawing a further distinction between the content of transactional records (e.g., a
29 check register or monthly statement) and the content of communications (e.g., a
30 phone call or email), with the Fourth Amendment only protecting the latter. But
31 there is no discussion of such a distinction in the cases.

32 In sum, there does not appear to be any clear Supreme Court authority for
33 limiting the third party doctrine to metadata. Nonetheless, there is one appellate
34 decision that seems to adopt such a rule. In *United States v. Forrester*,²² the Ninth
35 Circuit Court of Appeals held that the third party doctrine applies to government
36 collection of Internet metadata (including the addresses of all email messages sent
37 and received and all websites visited). In explaining its decision, the court asserted
38 that the Fourth Amendment protects content but does not protect metadata:

21. For an extended analysis of this proposition, see O. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 *Stan. L. Rev.* 1005 (2010).

22. 512 F. 3d 500 (9th Cir. 2008).

1 [Email] to/from addresses and IP addresses constitute addressing information
2 and do not necessarily reveal any more about the underlying contents of
3 communication than do phone numbers. When the government obtains the
4 to/from addresses of a person's e-mails or the IP addresses of websites visited, it
5 does not find out the contents of the messages or know the particular pages on the
6 websites the person viewed. At best, the government may make educated guesses
7 about what was said in the messages or viewed on the websites based on its
8 knowledge of the e-mail to/from addresses and IP addresses — but this is no
9 different from speculation about the contents of a phone conversation on the basis
10 of the identity of the person or entity that was dialed. Like IP addresses, certain
11 phone numbers may strongly indicate the underlying contents of the
12 communication; for example, the government would know that a person who
13 dialed the phone number of a chemicals company or a gun shop was likely
14 seeking information about chemicals or firearms. Further, when an individual
15 dials a pre-recorded information or subject-specific line, such as sports scores,
16 lottery results or phone sex lines, the phone number may even show that the caller
17 had access to specific content information. Nonetheless, the Court in *Smith* and
18 *Katz* drew a clear line between unprotected addressing information and protected
19 content information that the government did not cross here.²³

20 Finally, in *United States v. Warshak*,²⁴ the Sixth Circuit Court of Appeals held
21 that the Fourth Amendment protects the content of email messages, just as it does
22 the content of telephone calls and mailed letters. The court rejected an argument
23 that the third party doctrine defeats any reasonable expectation of privacy as to the
24 content of email. In doing so, the court did not discuss the distinction between
25 content and metadata. Instead, it emphasized that emails are voluntarily disclosed
26 to an Internet Service Provider solely for the purpose of transmission. The ISP acts
27 as a communication intermediary (which the court analogized to a telephone
28 company or the post office). It is not the intended recipient of the information.

29 That argument is sufficient to distinguish email from the bank records at issue in
30 *Miller* (where the bank was the intended recipient of the information contained in
31 the records). But it does not suffice to distinguish *Smith* (where the phone
32 company received telephone dialing information solely as a communication
33 intermediary).

34 In conclusion, there is an argument to be made that the third party doctrine does
35 not apply to the content of electronic communications, just as it does not apply to
36 the content of a telephone call. But the Supreme Court has not yet squarely
37 endorsed that position.

38 ***Recent Supreme Court Developments***

39 Although the Supreme Court has not modified the application of the third party
40 doctrine to modern electronic communications, there are some indications that it
41 may be prepared to do so.

23. *Id.* at 510-11 (emphasis added) (footnotes omitted).

24. 631 F.3d 266 (6th Cir. 2010).

1 In *United States v. Jones*,²⁵ a recent case involving location tracking devices,
2 Justice Sotomayor raised that possibility:

3 [It may be necessary to reconsider the premise that an individual has no
4 reasonable expectation of privacy in information voluntarily disclosed to third
5 parties. ... This approach is ill suited to the digital age, in which people reveal a
6 great deal of information about themselves to third parties in the course of
7 carrying out mundane tasks. People disclose the phone numbers that they dial or
8 text to their cellular providers; the URLs that they visit and the e-mail addresses
9 with which they correspond to their Internet service providers; and the books,
10 groceries, and medications they purchase to online retailers. Perhaps, as Justice
11 Alito notes, some people may find the “tradeoff” of privacy for convenience
12 “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” ...
13 and perhaps not. I for one doubt that people would accept without complaint the
14 warrantless disclosure to the Government of a list of every Web site they had
15 visited in the last week, or month, or year. But whatever the societal expectations,
16 they can attain constitutionally protected status only if our Fourth Amendment
17 jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not
18 assume that all information voluntarily disclosed to some member of the public
19 for a limited purpose is, for that reason alone, disintitiled to Fourth Amendment
20 protection.²⁶

21 In the same case, a concurrence joined by five justices strongly suggested that
22 there can be a reasonable expectation of privacy, for Fourth Amendment purposes,
23 with respect to location tracking information that is generated by a mobile
24 communication device.²⁷ That conclusion seems incompatible with the third party
25 doctrine; location tracking information is metadata that is disclosed voluntarily to
26 a third party service provider. If, as the concurrence maintains, the Fourth
27 Amendment applies to such information, then the third party doctrine must be
28 inapplicable.

29 More recently, the Court held that the Fourth Amendment applies to a police
30 search of the contents of a cell phone, incident to a lawful arrest.²⁸ As part of its
31 analysis, the Court analyzed the privacy expectations that a person has with
32 respect to the contents of a cell phone. In its analysis, the Court does not mention
33 that much of the information contained within a cell phone has been voluntarily
34 shared with third parties. Nor did it draw a clear distinction between content and
35 metadata. Significantly, the Court expressly rejected a government-proposed
36 exception to the warrant requirement for phone dialing information. Such an
37 exception would be easily administered and would seem to fall squarely within the
38 ambit of the existing third party doctrine. Importantly, such an exception would
39 have changed the results in one of the cases under review, which primarily

25. 132 S. Ct. 945 (2012).

26. *Id.* (Sotomayor, J., concurring).

27. *Id.* (Alito, J., concurring).

28. *Riley v. California*, 134 S. Ct. 2473 (2014).

1 involved access to phone dialing information. The fact that the Court chose not to
2 adopt the proposed exception casts doubt on the continued force of the third party
3 doctrine when applied to modern electronic communication information.

4 **Third Parties and Article I, Section 13 of the California Constitution**

5 As noted above, Article I, Section 13 of the California Constitution provides
6 protection that is very similar to the Fourth Amendment. However, there is one
7 important difference. The California Supreme Court has held that Article I,
8 Section 13 is not limited by an equivalent of the federal third party doctrine.

9 Before discussing that point further, it is worth discussing how Article I, Section
10 13 was affected by Proposition 8.

11 ***Proposition 8 – “Right to Truth-in-Evidence”***

12 In 1982, the voters approved Proposition 8, which added Article I, Section 28 of
13 the California Constitution. Among other things, Section 28 provides that the
14 People of California have the following right:

15 Right to Truth-in-Evidence. Except as provided by statute hereafter enacted by
16 a two-thirds vote of the membership in each house of the Legislature, relevant
17 evidence shall not be excluded in any criminal proceeding, including pretrial and
18 post conviction motions and hearings, or in any trial or hearing of a juvenile for a
19 criminal offense, whether heard in juvenile or adult court. Nothing in this section
20 shall affect any existing statutory rule of evidence relating to privilege or hearsay,
21 or Evidence Code Sections 352, 782 or 1103. Nothing in this section shall affect
22 any existing statutory or constitutional right of the press.²⁹

23 As a consequence of that new right, relevant evidence that is obtained in
24 violation of the California Constitution is nonetheless admissible in a criminal
25 proceeding, unless it falls within an exception to Section 28 or it was also obtained
26 in violation of the United States Constitution.³⁰ Consequently, evidence that is
27 obtained in violation of Article I, Section 13 cannot be excluded at trial, unless it
28 also violated the Fourth Amendment.

29 The California Supreme Court has made clear that Proposition 8 did not
30 eliminate the substantive right that is provided in Article I, Section 13.³¹ It simply
31 narrowed the remedies that are available to address a violation of that right:

32 What would have been an unlawful search or seizure in this state before the
33 passage of that initiative would be unlawful today, and this is so even if it would
34 pass muster under the federal constitution. What Proposition 8 does is to eliminate
35 a judicially created remedy for violations of the federal or state constitutions,

29. Cal. Const. art 1, § 28(f)(2).

30. In re Lance W., 37 Cal. 3d 873 (1985).

31. Proposition 115 (June 5, 1990), would have directly limited the scope of the rights provided by Article I, Section 13. The California Supreme Court held that it was improperly adopted and without effect. See *Raven v. Deukmejian*, 52 Cal. 3d 336 (1990).

1 through the exclusion of the evidence so obtained, except to the extent that
2 exclusion remains federally compelled.³²

3 For that reason, Article I, Section 13 continues to provide an independent
4 constitutional constraint on government searches. As discussed below, the
5 protection afforded by Article I, Section 13 is significantly greater than that
6 afforded by the Fourth Amendment.

7 ***Article I, Section 13 Is Not Subject to Third Party Doctrine***

8 In construing Article I, Section 13, the California Supreme Court has rejected
9 the federal third party doctrine.

10 In *Burrows v. Superior Court*,³³ the Court held that a person can have a
11 reasonable expectation of privacy with regard to that person’s bank records.

12 It cannot be gainsaid that the customer of a bank expects that the documents,
13 such as checks, which he transmits to the bank in the course of his business
14 operations, will remain private, and that such an expectation is reasonable. The
15 prosecution concedes as much, although it asserts that this expectation is not
16 constitutionally cognizable. Representatives of several banks testified at the
17 suppression hearing that information in their possession regarding a customer’s
18 account is deemed by them to be confidential.

19 ... A bank customer’s reasonable expectation is that, absent compulsion by
20 legal process, the matters he reveals to the bank will be utilized by the bank only
21 for internal banking purposes. Thus, we hold petitioner had a reasonable
22 expectation that the bank would maintain the confidentiality of those papers
23 which originated with him in check form and of the bank statements into which a
24 record of those same checks had been transformed pursuant to internal bank
25 practice.³⁴

26 The fact that the bank has a proprietary interest in its own records does not
27 affect the customer’s reasonable expectation of privacy:

28 The mere fact that the bank purports to own the records which it provided to the
29 detective is not, in our view, determinative of the issue at stake. The disclosure by
30 the depositor to the bank is made for the limited purpose of facilitating the
31 conduct of his financial affairs; it seems evident that his expectation of privacy is
32 not diminished by the bank’s retention of a record of such disclosures.³⁵

33 Furthermore, records of a customer’s financial transactions are an unavoidable
34 part of modern life, which provide a “virtual current biography” of the customer:

35 For all practical purposes, the disclosure by individuals or business firms of
36 their financial affairs to a bank is not entirely volitional, since it is impossible to

32. *Id.* at 886-87.

33. 13 Cal. 3d 238 (1974).

34. *Id.* at 243.

35. *Id.* at 244.

1 participate in the economic life of contemporary society without maintaining a
2 bank account. In the course of such dealings, a depositor reveals many aspects of
3 his personal affairs, opinions, habits and associations. Indeed, the totality of bank
4 records provides a virtual current biography. While we are concerned in the
5 present case only with bank statements, the logical extension of the contention
6 that the bank's ownership of records permits free access to them by any police
7 officer extends far beyond such statements to checks, savings, bonds, loan
8 applications, loan guarantees, and all papers which the customer has supplied to
9 the bank to facilitate the conduct of his financial affairs upon the reasonable
10 assumption that the information would remain confidential. To permit a police
11 officer access to these records merely upon his request, without any judicial
12 control as to relevancy or other traditional requirements of legal process, and to
13 allow the evidence to be used in any subsequent criminal prosecution against a
14 defendant, opens the door to a vast and unlimited range of very real abuses of
15 police power.

16 Cases are legion that condemn violent searches and invasions of an individual's
17 right to the privacy of his dwelling. The imposition upon privacy, although
18 perhaps not so dramatic, may be equally devastating when other methods are
19 employed. Development of photocopying machines, electronic computers and
20 other sophisticated instruments have accelerated the ability of government to
21 intrude into areas which a person normally chooses to exclude from prying eyes
22 and inquisitive minds. Consequently judicial interpretations of the reach of the
23 constitutional protection of individual privacy must keep pace with the perils
24 created by these new devices.³⁶

25 In *California v. Blair*,³⁷ the California Supreme Court extended the reasoning of
26 *Burrows* to records of credit card use and telephone numbers dialed. In both cases,
27 the defendant had a reasonable expectation of privacy under the California
28 Constitution:

29 The rationale of *Burrows* applies in a comparable manner to information
30 regarding charges made by a credit card holder. As with bank statements, a person
31 who uses a credit card may reveal his habits, his opinions, his tastes, and political
32 views, as well as his movements and financial affairs. No less than a bank
33 statement, the charges made on a credit card may provide "a virtual current
34 biography" of an individual. ...

35 A credit card holder would reasonably expect that the information about him
36 disclosed by those charges will be kept confidential unless disclosure is
37 compelled by legal process. The pervasive use of credit cards for an ever-
38 expanding variety of purposes — business, social, personal, familial — and the
39 intimate nature of the information revealed by the charges amply justify this
40 conclusion.³⁸

41 The same principle was found to be true for telephone number dialing records:

36. *Id.* at 247-48.

37. 25 Cal. 3d 640 (1979).

38. *Id.* at 652.

1 [A] telephone subscriber has a reasonable expectation that the calls he makes
2 will be utilized only for the accounting functions of the telephone company and
3 that he cannot anticipate that his personal life, as disclosed by the calls he makes
4 and receives, will be disclosed to outsiders without legal process. As with bank
5 records, concluded the court, it is virtually impossible for an individual or
6 business entity to function in the modern economy without a telephone, and a
7 record of telephone calls also provides “a virtual current biography.”³⁹

8 In *People v. Chapman*,⁴⁰ the court reaffirmed its reasoning in *Burrows* and *Blair*
9 and held that a person has a reasonable expectation of privacy with regard to a
10 name and address associated with an unlisted telephone number, notwithstanding
11 the fact that such information was voluntarily provided to the telephone company.

12 In summary, the cases discussed above state four main reasons why voluntarily
13 providing information to a third party for a limited purpose does not defeat a
14 reasonable expectation of privacy regarding that information:

- 15 • It is reasonable to assume that private information provided to a third party
16 will be used only for the limited purpose for which it is provided. The third
17 party will not disclose that information to outsiders (absent legal
18 compulsion).
- 19 • The fact that a third party professes a proprietary interest in information
20 provided by a customer does not affect the customer’s reasonable
21 expectation of privacy.
- 22 • In many cases, providing private information to a third party is “not entirely
23 volitional” because doing so is a practical necessity of modern life.
- 24 • Information provided to a third party for a limited purpose may reveal
25 “many aspects of [one’s] personal affairs, opinions, habits and associations,”
26 providing a “virtual current biography.” Such information is deserving of
27 protection from unreasonable government intrusion.

28 Importantly, these cases find that there can be a reasonable expectation of
29 privacy even with regard to metadata like telephone numbers dialed. If this is true
30 for metadata, then it must also be true for content (which provides a much richer
31 “virtual private biography” than is provided by telephone number dialing records
32 alone). This removes a major obstacle to applying Article I, Section 13 to modern
33 electronic communications.

34 **Additional Considerations in Special Cases**

35 *Interception of Communications*

36 In general, the Fourth Amendment requires that a search be authorized in
37 advance by a warrant that is issued by a neutral magistrate, based upon probable
38 cause. In addition, the warrant must particularly describe the place to be searched

39. *Id.* at 653.

40. 36 Cal. 3d 98 (1984).

1 and the person or things to be seized. The particularity requirements constrain the
2 scope of the search. Law enforcement is not free to search anywhere or to continue
3 searching after the items being sought have been found. Ordinarily, the person
4 whose privacy is invaded by a search receives contemporaneous notice of the
5 search.

6 Those general requirements pose special problems when applied to the
7 interception of communications (i.e., eavesdropping, wiretapping, or other
8 prospective interception of future communications). Interception involves a broad
9 and indiscriminate invasion of privacy, sweeping in both material and immaterial
10 information. The likelihood that interception will invade areas of privacy unrelated
11 to the purpose of the warrant increases with the duration of the interception, which
12 could be open-ended.

13 In *Berger v. New York*,⁴¹ the United States Supreme Court held that the
14 particularity requirements for an interception warrant are greater than those for a
15 regular search warrant. It is not sufficient to identify the person whose
16 communications will be intercepted.

17 [T]his does no more than identify the person whose constitutionally protected
18 area is to be invaded, rather than “particularly describing” the communications,
19 conversations, or discussions to be seized. As with general warrants, this leaves
20 too much to the discretion of the officer executing the order.⁴²

21 The Court also held that the period of interception must be limited and a new
22 showing of probable cause must be made to justify an extension. Otherwise, an
23 interception warrant would effectively authorize a series of searches, all grounded
24 on the original showing of probable cause.⁴³

25 Finally, the Court objected to the absence of notice to the target of the
26 interception, without some showing of exigency to justify the unconsented
27 intrusion. “Such a showing of exigency, in order to avoid notice, would appear
28 more important in eavesdropping, with its inherent dangers, than that required
29 when conventional procedures of search and seizure are utilized.”

30 In summary, an interception warrant must meet the general requirements for
31 issuance of a search warrant under the Fourth Amendment, and must also
32 particularly identify the communications that are being sought, limit the duration
33 of the interception (with a new showing of probable cause to justify an extension),
34 and demonstrate sufficient exigency to justify interception without notice to the
35 target of the interception. As discussed later in this report, these so-called “super-
36 warrant” requirements were codified in the federal wiretap statute.⁴⁴

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

42. *Id.* at 59.

43. *Id.* at 59-60.

44. See discussion of “Federal Statutory Law — Interception of Communications” *infra*.

1 **Location Tracking**

2 There are two general ways that communication service providers can track the
3 location of cell phones and other mobile communication devices:

- 4 (1) *Cell tower triangulation.* Cell service providers are able to approximate the
5 location of a cell phone, by applying a triangulation algorithm to data about
6 the phone’s communication with nearby cell towers.⁴⁵
- 7 (2) *Global positioning system (GPS) data.* Many cell phones and other mobile
8 communication devices are capable of determining the precise location of
9 the device by using the GPS satellite system.⁴⁶

10 The information used by service providers to determine the location of a mobile
11 communication device is metadata. It describes the status of the communication
12 device, without disclosing the content of any communication. It is also
13 information that is voluntarily disclosed to the communication provider. Thus,
14 location data would seem to fall squarely within the federal third party doctrine.

15 This suggests that there is no reasonable expectation of privacy with respect to
16 location data, sufficient to trigger the application of the Fourth Amendment.⁴⁷
17 However, as discussed above, the protection afforded by Article I, Section 13 of
18 the California Constitution is not limited by the third party doctrine. Therefore, a
19 person could have a reasonable expectation of privacy with regard to location
20 tracking information for the purposes of Article I, Section 13.

21 However, there is another potential limitation on a person’s reasonable
22 expectations of privacy with regard to location tracking. The United States
23 Supreme Court has held that a person does not have a reasonable expectation of
24 privacy as to the person’s movements within a public space. Such movements are
25 open to observation by any person, including police. “A person traveling in an
26 automobile on public thoroughfares has no reasonable expectation of privacy in

45. Congressional Research Service, *Governmental Tracking of Cell Phones and Vehicles: The Confluence of Privacy, Technology, and Law* at 8, n.60 (2011) (“There are two distinct technologies used to locate a cell phone through a network: time difference of arrival and the angle of arrival. ... The time difference technology measures the time it takes for a signal to travel from the cell phone to the tower. When multiple towers pick up this signal, an algorithm allows the network to determine the phone’s latitude and longitude. ... The angle of arrival technology uses the angles at which a phone’s signal reaches a station. When more than one tower receives the signal, the network compares this data the multiple angles of arrival and triangulates the location of the cell phone.”).

46. *Id.* (“GPS, or Global Positioning System, is a system of 24 satellites that constantly orbit Earth. ... When hardware inside the cell phone receives signals from at least four of these satellites, the handset can calculate its latitude and longitude to within 10 meters.”).

47. However, as discussed under “Recent Supreme Court Developments” *supra*, five justices of the United States Supreme Court have indicated, in *dicta*, that the Fourth Amendment does apply to location tracking of a sufficiently-long duration.

1 his movements from one place to another.”⁴⁸ That limitation on privacy does not
2 apply to information about a person’s location within private areas.⁴⁹

3 Notwithstanding the diminished expectation of privacy with regard to movement
4 in public areas, five Supreme Court Justices recently indicated, in *dicta*, that a
5 prolonged period of location tracking can violate reasonable expectations of
6 privacy under the Fourth Amendment.

7 The best that we can do in this case is to apply existing Fourth Amendment
8 doctrine and to ask whether the use of GPS tracking in a particular case involved
9 a degree of intrusion that a reasonable person would not have anticipated.

10 Under this approach, relatively short-term monitoring of a person’s movements
11 on public streets accords with expectations of privacy that our society has
12 recognized as reasonable. See *Knotts*.... But the use of longer term GPS
13 monitoring in investigations of most offenses impinges on expectations of
14 privacy. For such offenses, society’s expectation has been that law enforcement
15 agents and others would not — and indeed, in the main, simply could not secretly
16 monitor and catalogue every single movement of an individual’s car for a very
17 long period. In this case, for four weeks, law enforcement agents tracked every
18 movement that respondent made in the vehicle he was driving. We need not
19 identify with precision the point at which the tracking of this vehicle became a
20 search, for the line was surely crossed before the 4-week mark. Other cases may
21 present more difficult questions. But where uncertainty exists with respect to
22 whether a certain period of GPS surveillance is long enough to constitute a Fourth
23 Amendment search, the police may always seek a warrant. ... We also need not
24 consider whether prolonged GPS monitoring in the context of investigations
25 involving extraordinary offenses would similarly intrude on a constitutionally
26 protected sphere of privacy. In such cases, long-term tracking might have been
27 mounted using previously available techniques.

28 For these reasons, I conclude that the lengthy monitoring that occurred in this
29 case constituted a search under the Fourth Amendment.⁵⁰

30 Notably, the Court reached that conclusion even though location tracking
31 information is metadata that is voluntarily shared with a third party.

32 *Investigative Subpoena*

33 A warrant is not the only constitutionally sufficient authority to conduct a search
34 that is governed by the Fourth Amendment and Article I, Section 13 of the
35 California Constitution. In some circumstances, a search pursuant to an

48. United States v. Knotts, 460 U.S. 276, 281 (1983).

49. United States v. Karo, 468 U.S. 705, 714-15 (1984).

50. United States v. Jones, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring) (“I agree with Justice Alito that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’”).

1 investigative subpoena *duces tecum*,⁵¹ issued by a grand jury or an administrative
2 agency, can also be constitutionally reasonable.

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

6 [T]he Government cannot be required to justify the issuance of a grand jury
7 subpoena by presenting evidence sufficient to establish probable cause because
8 the very purpose of requesting the information is to ascertain whether probable
9 cause exists.⁵²

10 However, a grand jury subpoena must be reasonable. In *Hale v. Henkel*, the
11 Court held that a grand jury’s subpoena *duces tecum* was unreasonable under the
12 Fourth Amendment because it was “too sweeping in its terms” and violated “the
13 general principle of law with regard to the particularity required in the description
14 of documents necessary to a search warrant or subpoena.”⁵³

15 The same general principles apply to a subpoena *duces tecum* issued by an
16 administrative agency that is investigating a possible violation of the laws that it
17 enforces. The use of such a subpoena to compel the production of evidence (rather
18 than a warrant) does not violate the Fourth Amendment, so long as the subpoena is
19 authorized, sufficiently definite, and reasonable:

20 Insofar as the prohibition against unreasonable searches and seizures can be
21 said to apply at all it requires only that the inquiry be one which the agency
22 demanding production is authorized to make, that the demand be not too
23 indefinite, and that the information sought be reasonably relevant.⁵⁴

24 However, there may be a limitation on the constitutional use of an investigative
25 subpoena. Some courts have held that the constitutional reasonableness of a search
26 pursuant to a subpoena *duces tecum* depends on the fact that the person whose
27 records would be searched has notice and an opportunity for judicial review before
28 any records are actually seized.

29 While the Fourth Amendment protects people “against unreasonable searches
30 and seizures,” it imposes a probable cause requirement only on the issuance of
31 warrants. Thus, unless subpoenas are warrants, they are limited by the general
32 reasonableness standard of the Fourth Amendment (protecting the people against
33 “unreasonable searches and seizures”), not by the probable cause requirement.

51. This report does not consider the use of a subpoena as an instrument of discovery in a pending adjudicative proceeding.

52. *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991).

53. 201 U.S. 43, 76-77 (1906).

54. *Brovelli v. Superior Court*, 56 Cal. 2d 524, 529 (1961) (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 651-54 (1950)); see also *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.”).

1 A warrant is a judicial authorization to a law enforcement officer to search or
2 seize persons or things. To preserve advantages of speed and surprise, the order is
3 issued without prior notice and is executed, often by force, with an unannounced
4 and unanticipated physical intrusion. Because this intrusion is both an immediate
5 and substantial invasion of privacy, a warrant may be issued only by a judicial
6 officer upon a demonstration of probable cause — the safeguard required by the
7 Fourth Amendment.

8 *A subpoena, on the other hand, commences an adversary process during which*
9 *the person served with the subpoena may challenge it in court before complying*
10 *with its demands. As judicial process is afforded before any intrusion occurs, the*
11 *proposed intrusion is regulated by, and its justification derives from, that process.*

12 In short, the immediacy and intrusiveness of a search and seizure conducted
13 pursuant to a warrant demand the safeguard of demonstrating probable cause to a
14 neutral judicial officer before the warrant issues, whereas the issuance of a
15 subpoena initiates an adversary process that can command the production of
16 documents and things only after judicial process is afforded. And while a
17 challenge to a warrant questions the actual search or seizure under the probable
18 cause standard, a challenge to a subpoena is conducted through the adversarial
19 process, questioning the reasonableness of the subpoena’s command.⁵⁵

20 Advance notice and an opportunity for judicial review before records are
21 searched are a routine feature of the procedure for issuance and execution of an
22 investigative subpoena *duces tecum*,⁵⁶ when the subpoena is used to search records
23 that are held by the person whose records are to be searched. But when a subpoena
24 is instead served on a third party service provider, to search a customer’s records,
25 that customer may not receive any notice of the search or an opportunity for
26 judicial review of the constitutionality of the search. In such a situation, only the
27 service provider has an opportunity for judicial review of the subpoena. The
28 service provider is not an adequate surrogate to protect the interests of the
29 customer. The service provider may have no reason to object to the search, is
30 usually shielded from liability for complying with the subpoena, and in some
31 circumstances, may be legally prohibited from notifying the customer.⁵⁷

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

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

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

57. See, e.g., 18 U.S.C. § 2705(b).

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

3 **Summary of Search and Seizure Requirements**

4 *Electronic communications generally protected.* The Fourth Amendment and
5 Article I, Section 13 of the California Constitution protect a person’s reasonable
6 expectations of privacy with regard to that person’s electronic communications.

7 *Third party doctrine limits Fourth Amendment protections.* Under the Fourth
8 Amendment, there is no reasonable expectation of privacy with regard to
9 information that is voluntarily provided to a third party. There are some
10 indications that this third party doctrine may only apply to metadata (i.e., it does
11 not apply to the content of communications), but that is not certain. There are also
12 indications that the United States Supreme Court may be moving toward
13 reconsideration of the third party doctrine with regard to modern electronic
14 communications, but it has not yet done so.

15 *Third party doctrine inapplicable to the California Constitution.* Article I,
16 Section 13 of the California Constitution is not subject to the third party doctrine.
17 The California Supreme Court has held that there can be a reasonable expectation
18 of privacy with respect to information disclosed to a third party, where the
19 disclosure is not truly volitional (because it is a practical necessity of modern life);
20 where the information was provided for a limited purpose, with an expectation that
21 it will not be shared with others (absent legal compulsion); and where the
22 information would provide details about a person’s private life akin to a “virtual
23 current biography.” Such information includes bank records, telephone numbers
24 dialed, credit card transaction data, and the identity of a person associated with an
25 unlisted telephone number.

26 *Interception of communications subject to “super-warrant” requirements.* The
27 interception of communications poses special problems with respect to the
28 requirements of the Fourth Amendment. Interception could invade the privacy of
29 communications that are beyond the scope of the authority provided in a warrant.
30 An interception of long duration could be the equivalent of a series of searches,
31 with a finding of probable cause only as to the first. Interception without notice to
32 the subject of the interception requires some showing of exigency. Those problems
33 require the inclusion of special limitations in an interception warrant. Such “super-
34 warrant” limitations have been codified in the federal wiretap statute.⁵⁸

35 *Movement in public areas.* A person has a diminished expectation of privacy
36 with regard to the person’s movements in public areas. For that reason, location
37 tracking within public areas may not be a search within the meaning of the Fourth

58. See discussion of “Federal Statutory Law — Interception of Communications” *infra*.

1 Amendment. However, continuous location tracking for an extended period (e.g.,
2 four weeks) would likely be considered a search under the Fourth Amendment.

3 *Investigative subpoena.* Under the Fourth Amendment and Article I, Section 13
4 of the California Constitution, an investigative subpoena *duces tecum* issued by a
5 grand jury or administrative agency may provide sufficient authority to conduct a
6 constitutionally reasonable records search. The standard for review of such a
7 subpoena examines whether it is lawfully issued, whether it is too indefinite, and
8 whether the information sought is reasonably relevant to its purpose. When a
9 subpoena is served on the person whose records will be searched, that person has
10 notice and an opportunity for judicial review of the constitutionality of the search,
11 before any records are seized. Some courts suggest that this notice and an
12 opportunity for judicial review is essential to the constitutional reasonableness of
13 the use of an investigative subpoena, rather than a warrant. If that is correct, the
14 service of an investigative subpoena on a third party service provider, without
15 notice to the customer whose records are to be searched, may not be sufficient.
16 That issue has not been squarely decided.

17 Freedom of Expression

18 The First Amendment to the United States Constitution expressly protects the
19 freedom of speech:

20 Congress shall make no law respecting an establishment of religion, or
21 prohibiting the free exercise thereof; or abridging the freedom of speech, or of the
22 press; or the right of the people peaceably to assemble, and to petition the
23 Government for a redress of grievances.

24 The First Amendment is applicable to the states.⁵⁹

25 The California Constitution also expressly protects freedom of speech, in Article
26 I, Section 2(a):

27 Every person may freely speak, write and publish his or her sentiments on all
28 subjects, being responsible for the abuse of this right. A law may not restrain or
29 abridge liberty of speech or press.

30 Government surveillance of electronic communications does not directly restrain
31 speech or association. However, such surveillance could indirectly affect
32 expression, in ways that can violate free expression rights. “Freedoms such as

59. *Near v. Minnesota*, 283 U.S. 697, 707 (1931) (“It is no longer open to doubt that the liberty of the press, and of speech, is within the liberty safeguarded by the due process clause of the Fourteenth Amendment from invasion by state action. It was found impossible to conclude that this essential personal liberty of the citizen was left unprotected by the general guaranty of fundamental rights of person and property.”).

1 these are protected not only against heavy-handed frontal attack, but also from
2 being stifled by more subtle governmental interference.”⁶⁰

3 This report discusses five ways in which government surveillance of electronic
4 communications could indirectly restrain free speech or association:

- 5 (1) *Associational privacy*. The Internet enables the formation of private groups
6 for the discussion and advancement of ideas. If the government can
7 determine the identity of the participants in an online discussion forum, it
8 could chill the free association of those who wish to “gather” online for the
9 purpose of private group discussions.
- 10 (2) *Anonymous speech*. The Internet makes it very easy for a person to make
11 public statements anonymously. If the government can determine the
12 identity of a person associated with an anonymous user name on an Internet
13 discussion forum, that could chill the free expression of those who are only
14 comfortable speaking anonymously.
- 15 (3) *Reader privacy*. The Internet is an extremely important source of
16 information and opinion. If the government can access a person’s
17 communication data, it could determine what content a person has been
18 reading or viewing. This invasion of a reader’s privacy could chill the right
19 to read unpopular or embarrassing material.
- 20 (4) *Private speech*. Electronic communications are an increasingly important
21 conduit for protected speech. If government is known to directly monitor
22 electronic communications, that surveillance could have a chilling effect on
23 expressive activity.
- 24 (5) *Press confidentiality*. Increasingly, journalists are using the Internet, both as
25 a place to publish and a tool for research and for confidential
26 communication with sources. Government access to a journalist’s private
27 electronic communications could reveal confidential sources and methods,
28 chilling press freedom.

29 **Associational Privacy**

30 In *National Association for the Advancement of Colored People v. Alabama*,⁶¹ a
31 discovery order required the NAACP to produce a full list of its Alabama
32 membership. The NAACP refused to do so and was found to be in contempt. The
33 matter was eventually appealed to the United States Supreme Court, which held
34 that compelled production of the group’s membership list would
35 unconstitutionally infringe on the members’ rights of free association.

36 The Court first explained that the Constitution protects the right of free
37 association, which is enforceable against the states under the Fourteenth
38 Amendment:

39 Effective advocacy of both public and private points of view, particularly
40 controversial ones, is undeniably enhanced by group association, as this Court has

60. *Bates v. Little Rock*, 361 U.S. at 523.

61. 357 U.S. 449 (1958) (hereafter “NAACP v. Alabama”).

1 more than once recognized by remarking upon the close nexus between the
2 freedoms of speech and assembly. ... It is beyond debate that freedom to engage
3 in association for the advancement of beliefs and ideas is an inseparable aspect of
4 the “liberty” assured by the Due Process Clause of the Fourteenth Amendment,
5 which embraces freedom of speech. ... Of course, it is immaterial whether the
6 beliefs sought to be advanced by association pertain to political, economic,
7 religious or cultural matters, and state action which may have the effect of
8 curtailing the freedom to associate is subject to the closest scrutiny.⁶²

9 The Court then explained that government invasion of the privacy of group
10 affiliation can indirectly violate the right of free association:

11 The fact that Alabama, so far as is relevant to the validity of the contempt
12 judgment presently under review, has taken no direct action ... to restrict the right
13 of petitioner’s members to associate freely, does not end inquiry into the effect of
14 the production order. ... In the domain of these indispensable liberties, whether of
15 speech, press, or association, the decisions of this Court recognize that abridgment
16 of such rights, even though unintended, may inevitably follow from varied forms
17 of governmental action. Thus in [*American Communications Assn. v. Douds*, 339
18 U.S. 382 (1950)], the Court stressed that the legislation there challenged, which
19 on its face sought to regulate labor unions and to secure stability in interstate
20 commerce, would have the practical effect “of discouraging” the exercise of
21 constitutionally protected political rights, ... and it upheld the statute only after
22 concluding that the reasons advanced for its enactment were constitutionally
23 sufficient to justify its possible deterrent effect upon such freedoms. Similar
24 recognition of possible unconstitutional intimidation of the free exercise of the
25 right to advocate underlay this Court’s narrow construction of the authority of a
26 congressional committee investigating lobbying and of an Act regulating
27 lobbying, although in neither case was there an effort to suppress speech. ... The
28 governmental action challenged may appear to be totally unrelated to protected
29 liberties. Statutes imposing taxes upon rather than prohibiting particular activity
30 have been struck down when perceived to have the consequence of unduly
31 curtailing the liberty of freedom of press assured under the Fourteenth
32 Amendment.

33 It is hardly a novel perception that compelled disclosure of affiliation with
34 groups engaged in advocacy may constitute as effective a restraint on freedom of
35 association as the forms of governmental action in the cases above were thought
36 likely to produce upon the particular constitutional rights there involved. This
37 Court has recognized the vital relationship between freedom to associate and
38 privacy in one’s associations. When referring to the varied forms of governmental
39 action which might interfere with freedom of assembly, it said in *American*
40 *Communications Assn. v. Douds*...: “A requirement that adherents of particular
41 religious faiths or political parties wear identifying arm-bands, for example, is
42 obviously of this nature.” Compelled disclosure of membership in an organization
43 engaged in advocacy of particular beliefs is of the same order. Inviolability of
44 privacy in group association may in many circumstances be indispensable to

62. *NAACP v. Alabama*, 357 U.S. at 460-61.

1 preservation of freedom of association, particularly where a group espouses
2 dissident beliefs.⁶³

3 Based on that reasoning, the Court held that the state court order compelling
4 production of the NAACP’s membership list “must be regarded as entailing the
5 likelihood of a substantial restraint upon the exercise by petitioner’s members of
6 their right to freedom of association.”⁶⁴ Such a restraint must be justified by a
7 compelling state interest.⁶⁵

8 It is easy to foresee situations in which government surveillance of electronic
9 communications could invade the right of associational privacy. The Internet has
10 become an important extension of the public square and many advocacy
11 organizations will “meet” to discuss their business in private online groups. A
12 government demand that a communication service provider disclose the identities
13 of the members of an online discussion group could have the same kind of
14 deleterious effect on association and expression that was at issue in *NAACP v.*
15 *Alabama*.

16 It is also possible that location tracking data could be used to invade
17 associational privacy. For example, if the government knows that a particular
18 group will be meeting in a certain building at a certain time, location tracking data
19 could be used to determine who is present at the time of the meeting.⁶⁶

20 **Anonymous Speech**

21 In *Talley v. California*,⁶⁷ the United States Supreme Court held that the right of
22 free expression includes the right to speak anonymously.⁶⁸ The case involved a
23 municipal ordinance that forbade the distribution of any handbill that did not state
24 the name and address of the person who prepared, distributed, or sponsored it.

25 The Court first discussed prior cases in which it held that a complete prohibition
26 on the public distribution of printed literature violated the constitutional right of
27 freedom of speech.⁶⁹ It then considered whether a narrower prohibition, on the
28 distribution of *anonymous* literature, would be constitutional.

63. *Id.* at 461-62.

64. *Id.* at 462.

65. *Id.* at 463.

66. For example, it has been reported that the National Security Agency collects billions of bits of cell phone location data daily, and uses the information to “infer relationships” between co-located persons. <<http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/>>

67. 362 U.S. 60 (1960).

68. See also *Huntley v. Public Utilities Com.*, 69 Cal. 2d 67 (1968) (invalidating requirement that recorded messages identify their source).

69. *Id.* at 62-63.

1 The Court had “no doubt” that requiring the source of a pamphlet to be
2 identified “would tend to restrict freedom to distribute information and therefore
3 freedom of expression.”⁷⁰

4 Anonymous pamphlets, leaflets, brochures and even books have played an
5 important role in the progress of mankind. Persecuted groups and sects from time
6 to time throughout history have been able to criticize oppressive practices and
7 laws either anonymously or not at all. The obnoxious press licensing law of
8 England, which was also enforced on the Colonies, was due in part to the
9 knowledge that exposure of the names of printers, writers and distributors would
10 lessen the circulation of literature critical of the government. The old seditious
11 libel cases in England show the lengths to which government had to go to find out
12 who was responsible for books that were obnoxious to the rulers. John Lilburne
13 was whipped, pilloried and fined for refusing to answer questions designed to get
14 evidence to convict him or someone else for the secret distribution of books in
15 England. Two Puritan Ministers, John Penry and John Udal, were sentenced to
16 death on charges that they were responsible for writing, printing or publishing
17 books. ... Before the Revolutionary War colonial patriots frequently had to
18 conceal their authorship or distribution of literature that easily could have brought
19 down on them prosecutions by English-controlled courts. Along about that time
20 the Letters of Junius were written and the identity of their author is unknown to
21 this day. ... Even the Federalist Papers, written in favor of the adoption of our
22 Constitution, were published under fictitious names. It is plain that anonymity has
23 sometimes been assumed for the most constructive purposes.

24 We have recently had occasion to hold in two cases that there are times and
25 circumstances when States may not compel members of groups engaged in the
26 dissemination of ideas to be publicly identified. *Bates v. Little Rock*, 361 U.S.
27 516; *N. A. A. C. P. v. Alabama*, 357 U.S. 449, 462. The reason for those holdings
28 was that identification and fear of reprisal might deter perfectly peaceful
29 discussions of public matters of importance. This broad Los Angeles ordinance is
30 subject to the same infirmity. We hold that it, like the Griffin, Georgia, ordinance
31 [generally prohibiting the public distribution of printed literature], is void on its
32 face.⁷¹

33 The Internet provides an ideal forum for anonymous speech. There are many
34 public and private discussion sites that support the use of pseudonyms. If state or
35 local agencies could access the customer records of the entities that maintain such
36 sites, they could learn the true identity of those who have chosen to speak
37 anonymously. While that would not prohibit or punish anonymous speech, it could
38 well deter it.

70. *Id.* at 64.

71. *Id.* at 65 (footnotes omitted). See also *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995) (“Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. ... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation — and their ideas from suppression — at the hand of an intolerant society.”).

1 **Reader Privacy**

2 The right of free speech includes the right to receive and read the speech of
3 others.⁷² And, just as the Constitution protects anonymous speech, the Constitution
4 also protects a right of privacy as to what one reads.

5 In *United States v. Rumely*,⁷³ the Court was presented with the question of
6 whether a congressional investigating committee could constitutionally compel a
7 publisher to disclose the identities of those who bought certain books. The Court
8 did not ultimately answer that question, deciding the case on other grounds,⁷⁴ but a
9 concurring opinion authored by Justice Douglas provides a cogent argument in
10 favor of constitutional protection of reader privacy:

11 If the present inquiry were sanctioned, the press would be subjected to
12 harassment that in practical effect might be as serious as censorship. A publisher,
13 compelled to register with the Federal Government, would be subjected to
14 vexatious inquiries. A requirement that a publisher disclose the identity of those
15 who buy his books, pamphlets, or papers is indeed the beginning of surveillance
16 of the press. True, no legal sanction is involved here. Congress has imposed no
17 tax, established no board of censors, instituted no licensing system. But the
18 potential restraint is equally severe. The finger of government leveled against the
19 press is ominous. Once the government can demand of a publisher the names of
20 the purchasers of his publications, the free press as we know it disappears. Then
21 the spectre of a government agent will look over the shoulder of everyone who
22 reads. The purchase of a book or pamphlet today may result in a subpoena
23 tomorrow. Fear of criticism goes with every person into the bookstall. The subtle,
24 imponderable pressures of the orthodox lay hold. Some will fear to read what is
25 unpopular, what the powers-that-be dislike. When the light of publicity may reach
26 any student, any teacher, inquiry will be discouraged. The books and pamphlets
27 that are critical of the administration, that preach an unpopular policy in domestic
28 or foreign affairs, that are in disrepute in the orthodox school of thought will be
29 suspect and subject to investigation. The press and its readers will pay a heavy
30 price in harassment. But that will be minor in comparison with the menace of the
31 shadow which government will cast over literature that does not follow the
32 dominant party line. If the lady from Toledo can be required to disclose what she
33 read yesterday and what she will read tomorrow, fear will take the place of
34 freedom in the libraries, book stores, and homes of the land. Through the

72. *Stanley v. Georgia*, 394 U.S. 557, 565 (1969) (“If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.”). See also *Lamont v. Postmaster General*, 381 U.S. 301, 307-08 (Brennan, J., concurring) (“I think the right to receive publications is such a fundamental right. The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.”).

73. 345 U.S. 41 (1953).

74. *Id.* at 47 (“Grave constitutional questions are matters properly to be decided by this Court but only when they inescapably come before us for adjudication. Until then it is our duty to abstain from marking the boundaries of congressional power or delimiting the protection guaranteed by the First Amendment. Only by such self-restraint will we avoid the mischief which has followed occasional departures from the principles which we profess.”).

1 harassment of hearings, investigations, reports, and subpoenas government will
2 hold a club over speech and over the press. Congress could not do this by law.⁷⁵

3 A few years later, in *Lamont v. Postmaster General*,⁷⁶ the Supreme Court
4 considered the constitutionality of a statute requiring that persons file a formal
5 request with the Postal Service as a prerequisite to receiving certain “communist
6 propaganda” by mail. In effect, this required recipients of such material to
7 expressly affirm to the government their interest in reading it.

8 The Court found the statute to violate the *recipient’s* constitutional right of free
9 speech:

10 This amounts in our judgment to an unconstitutional abridgment of the
11 addressee’s First Amendment rights. The addressee carries an affirmative
12 obligation which we do not think the Government may impose on him. This
13 requirement is almost certain to have a deterrent effect, especially as respects
14 those who have sensitive positions. Their livelihood may be dependent on a
15 security clearance. Public officials, like schoolteachers who have no tenure, might
16 think they would invite disaster if they read what the Federal Government says
17 contains the seeds of treason. Apart from them, any addressee is likely to feel
18 some inhibition in sending for literature which federal officials have condemned
19 as “communist political propaganda.” The regime of this Act is at war with the
20 “uninhibited, robust, and wide-open” debate and discussion that are contemplated
21 by the First Amendment.⁷⁷

22 Although the Court did not expressly state that it was concerned about the right
23 to *privacy* as to what one reads, that concern is plainly implicit in the passage
24 quoted above. If citizens must inform the government of the material that they
25 read, that requirement could have a significant chilling effect on the exercise of the
26 right to read unpopular materials.

27 The Internet is an important source of news and opinion. If the government were
28 able to access customer records of communication service providers, it would in
29 some cases be able to determine what a person has been reading or is interested in
30 reading. For example, access to a customer’s Internet meta-data might reveal:

- 31 • What websites the person has visited.
32 • What search terms a person has used when conducting online searches.
33 • What PDF files or e-books a person has downloaded.
34 • What image files or videos a person has viewed.

35 While government access to that type of information would not directly bar a
36 person from accessing particular Internet content, it could have a chilling effect
37 that would deter a person from fully exercising the constitutionally protected right

75. *Id.* at 56-58 (Douglas, J., concurring).

76. 381 U.S. 301.

77. *Id.* at 307.

1 to read what one pleases. This is especially likely where the content at issue is
2 controversial, unpopular, or embarrassing.

3 **Private Speech**

4 In *White v. Davis*,⁷⁸ the California Supreme Court considered the
5 constitutionality of a Los Angeles Police Department operation that involved the
6 use of undercover agents, posing as college students, who attended classes in order
7 to collect intelligence on student dissidents and their professors. There was no
8 allegation that the police were investigating illegal activity or acts. The undercover
9 surveillance was challenged on a number of grounds, including an assertion that it
10 violated the constitutional rights of free speech and association.⁷⁹

11 While the Court recognized that the surveillance program did not directly
12 prohibit speech or association, nonetheless “such surveillance may still run afoul
13 of the constitutional guarantee if the effect of such activity is to chill
14 constitutionally protected activity.”⁸⁰ The Court found that the police surveillance
15 at issue could have such an effect:

16 As a practical matter, the presence in a university classroom of undercover
17 officers taking notes to be preserved in police dossiers must inevitably inhibit the
18 exercise of free speech both by professors and students. In a line of cases
19 stretching over the past two decades, the United States Supreme Court has
20 repeatedly recognized that to compel an individual to disclose his political ideas
21 or affiliations to the government is to deter the exercise of First Amendment
22 rights.⁸¹

23 The fact that the students and professors were sharing their ideas in a setting that
24 was partially accessible to the public did not alter the Court’s conclusion:

25 Although defendant contends that the “semi-public” nature of a university
26 classroom negates any claim of “First Amendment privacy,” the controlling
27 Supreme Court rulings refute this assertion. For example, in both *N.A.A.C.P.* and
28 *Talley*, the fact that the private individuals involved had revealed their
29 associations or beliefs to many people was not viewed by the court as curtailing
30 their basic interest in preventing *the government* from prying into such matters.
31 Although if either a teacher or student speaks in class he takes the “risk” that
32 another class member will take note of the statement and perhaps recall it in the
33 future, such a risk is qualitatively different than that posed by a governmental
34 surveillance system involving the filing of reports in permanent police records.

78. 13 Cal. 3d 757 (1975).

79. For a discussion of whether the undercover operation violated the right of privacy under the California Constitution, see Memorandum 2014-21, pp. 12-14.

80. *White v. Davis*, 13 Cal. 3d at 767.

81. *Id.* at 767-68.

1 The greatly increased “chilling effect” resulting from the latter *governmental*
2 activity brings constitutional considerations into play.⁸²

3 The Court held that the surveillance of protected speech could pose “such a
4 grave threat to freedom of expression” that the “government bears the
5 responsibility of demonstrating a compelling state interest which justifies such
6 impingement and of showing that its purposes cannot be achieved by less
7 restrictive means.”⁸³

8 Subsequent federal appellate decisions suggest that a “legitimate law
9 enforcement purpose” can be sufficient to justify the surveillance of protected
10 speech, provided that the government is acting in good faith, without the actual
11 purpose of violating First Amendment rights.⁸⁴

12 **Press Confidentiality**

13 Government surveillance of a journalist’s electronic communications could
14 indirectly chill press freedoms. For example, in *Zurcher v. Stanford Daily*⁸⁵ police
15 searched a college newspaper’s offices for photographs that might reveal the
16 identity of demonstrators who had assaulted police. The *Stanford Daily* objected to
17 the search, in part on the ground that it violated its First Amendment rights in a
18 number of ways:

19 First, searches will be physically disruptive to such an extent that timely
20 publication will be impeded. Second, confidential sources of information will dry
21 up, and the press will also lose opportunities to cover various events because of
22 fears of the participants that press files will be readily available to the authorities.
23 Third, reporters will be deterred from recording and preserving their recollections
24 for future use if such information is subject to seizure. Fourth, the processing of
25 news and its dissemination will be chilled by the prospects that searches will
26 disclose internal editorial deliberations. Fifth, the press will resort to self-
27 censorship to conceal its possession of information of potential interest to the
28 police.⁸⁶

29 The Court seems to have conceded the seriousness of those concerns. But it held
30 that the Fourth Amendment provides adequate protection, balancing the
31 government’s legitimate interest in conducting a search based on a narrowly
32 drawn criminal warrant against the effects that such a search could have on press
33 freedom:

82. *Id.* at 768 n.4 (emphasis in original).

83. *Id.* at 760-61.

84. *United States v. Mayer*, 503 F.3d 740 (9th Cir. 2007); *United States v. Aguilar*, 883 F.2d 662 (9th Cir. 1989).

85. 436 U.S. 547 (1978).

86. *Id.* at 563-64.

1 Properly administered, the preconditions for a warrant — probable cause,
2 specificity with respect to the place to be searched and the things to be seized, and
3 overall reasonableness — should afford sufficient protection against the harms
4 that are assertedly threatened by warrants for searching newspaper offices.

5 ...

6 The hazards of such warrants can be avoided by a neutral magistrate carrying
7 out his responsibilities under the Fourth Amendment, for he has ample tools at his
8 disposal to confine warrants to search within reasonable limits.⁸⁷

9 The *Zurcher* decision was controversial.⁸⁸ It was quickly superseded by
10 legislation, at both the federal and state level, strictly limiting government’s ability
11 to search journalist records.⁸⁹

12 **Conclusion**

13 There are a number of ways in which government surveillance of electronic
14 communications could indirectly restrain free expression. It could breach the
15 privacy of group affiliation, the right to speak anonymously, and the right to
16 reader privacy. Surveillance of electronic communications could also chill
17 unpopular speech and could adversely affect press freedoms by revealing
18 confidential information about press sources and methods.

19 Although *Zurcher* was superseded by legislation, the holding in that case
20 suggests one way that surveillance of electronic communications could be
21 conducted without violating First Amendment rights — through use of a search
22 warrant that satisfies the requirements of the Fourth Amendment. As discussed
23 above, such a warrant is already required when police conduct surveillance of
24 communications.

25 Privacy

26 **“Penumbral” Privacy Right in the United States Constitution**

27 The United States Constitution does not contain express language guaranteeing a
28 general right of privacy. However, there are several cases in which the Supreme
29 Court has found a constitutional right of privacy, either in the “penumbra” of other
30 enumerated constitutional rights, as a liberty interest protected as a matter of
31 substantive due process, or as a right that preceded the Constitution and is
32 preserved by the Ninth Amendment.

87. *Id.* at 565-67.

88. See, e.g., Erburu, *Zurcher v. Stanford Daily: the Legislative Debate*, 17 Harv. J. on Legis. 152 (1980) (“Few decisions in the modern history of the Supreme Court have engendered as vociferous and uniformly unfavorable a response from advocates of a free press as the 1978 decision in *Zurcher v. Stanford Daily*.”).

89. See 42 U.S.C. § 2000aa (Privacy Protection Act of 1980, discussed at text accompanying notes 319-27 *infra*); Penal Code § 1524(g) (discussed under “Brief List of California Privacy Statutes” *infra*).

1 For example, in *Griswold v. Connecticut*,⁹⁰ the court found that a state law
2 criminalizing the use of birth control violated a constitutional right of marital
3 privacy. In reaching that conclusion, the Court noted earlier decisions that had
4 found unexpressed constitutional rights in the “penumbras” of specifically
5 enumerated rights:

6 The association of people is not mentioned in the Constitution nor in the Bill of
7 Rights. The right to educate a child in a school of the parents’ choice — whether
8 public or private or parochial — is also not mentioned. Nor is the right to study
9 any particular subject or any foreign language. Yet the First Amendment has been
10 construed to include certain of those rights.

11 ...

12 The foregoing cases suggest that specific guarantees in the Bill of Rights have
13 penumbras, formed by emanations from those guarantees that help give them life
14 and substance. ... Various guarantees create zones of privacy. The right of
15 association contained in the penumbra of the First Amendment is one, as we have
16 seen. The Third Amendment in its prohibition against the quartering of soldiers
17 “in any house” in time of peace without the consent of the owner is another facet
18 of that privacy. The Fourth Amendment explicitly affirms the “right of the people
19 to be secure in their persons, houses, papers, and effects, against unreasonable
20 searches and seizures.” The Fifth Amendment in its Self-Incrimination Clause
21 enables the citizen to create a zone of privacy which government may not force
22 him to surrender to his detriment. The Ninth Amendment provides: “The
23 enumeration in the Constitution, of certain rights, shall not be construed to deny
24 or disparage others retained by the people.”⁹¹

25 The exact character and scope of the federal constitutional privacy right is
26 difficult to describe with certainty. One source of difficulty is the inconsistency in
27 discussing the source of the privacy right. Another is the fact that the term
28 “privacy” has been used to describe two distinctly different concepts:

29 The cases sometimes characterized as protecting “privacy” have in fact
30 involved at least two different kinds of interests. One is the individual interest in
31 avoiding disclosure of personal matters, and another is the interest in
32 independence in making certain kinds of important decisions.⁹²

33 Said another way:

34 The former interest is informational or data-based; the latter involves issues of
35 personal freedom of action and autonomy in individual encounters with
36 government. The distinction between the two interests is not sharply drawn —
37 disclosure of information, e.g., information about one’s financial affairs, may
38 have an impact on personal decisions and relationships between individuals and
39 government.⁹³

90. 381 U.S. 479 (1965).

91. *Id.* at 482-84.

92. *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) (footnotes omitted).

93. *Hill v. Nat. Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 30 (1994).

1 The California Supreme Court has described those two types of privacy interests
2 as “informational privacy” and “autonomy privacy,” respectively:

3 Legally recognized privacy interests are generally of two classes: (1) interests
4 in precluding the dissemination or misuse of sensitive and confidential
5 information (“informational privacy”); and (2) interests in making intimate
6 personal decisions or conducting personal activities without observation,
7 intrusion, or interference (“autonomy privacy”).⁹⁴

8 *Autonomy Privacy*

9 Most of the Supreme Court decisions finding a constitutional privacy right
10 involve autonomy privacy. They address an individual’s right to make decisions
11 about important personal matters, free from government interference:

12 Although “[t]he Constitution does not explicitly mention any right of privacy,”
13 the Court has recognized that one aspect of the “liberty” protected by the Due
14 Process Clause of the Fourteenth Amendment is “a right of personal privacy, or a
15 guarantee of certain areas or zones of privacy.” *Roe v. Wade*, 410 U.S. 113, 152
16 (1973). This right of personal privacy includes “the interest in independence in
17 making certain kinds of important decisions.” *Whalen v. Roe*, 429 U.S. 589, 599-
18 600 (1977). While the outer limits of this aspect of privacy have not been marked
19 by the Court, it is clear that among the decisions that an individual may make
20 without unjustified government interference are personal decisions “relating to
21 marriage, *Loving v. Virginia*, 388 U.S. 1, 12 (1967); procreation, *Skinner v.*
22 *Oklahoma ex rel. Williamson*, 316 U.S. 535, 541-542 (1942); contraception,
23 *Eisenstadt v. Baird*, 405 U.S., at 453-454; *id.*, at 460, 463-465 (WHITE, J.,
24 concurring in result); family relationships, *Prince v. Massachusetts*, 321 U.S. 158,
25 166 (1944); and child rearing and education, *Pierce v. Society of Sisters*, 268 U.S.
26 510, 535 (1925); *Meyer v. Nebraska*, [262 U.S. 390, 399 (1923)].” *Roe v. Wade*,
27 *supra*, at 152-153.⁹⁵

28 The right of autonomy privacy does not seem to have direct relevance to
29 government surveillance of electronic communications, because surveillance does
30 not prohibit or restrict choice in the areas protected by autonomy privacy.

31 However, electronic surveillance could have an indirect effect on autonomy
32 privacy, if government collection of private information would deter the exercise
33 of personal liberty. For example, in *Whalen v. Roe*,⁹⁶ a New York statute
34 authorized the government to collect information about medical prescriptions for
35 specified drugs. Appellees argued that this program would violate both
36 informational privacy rights (by collecting private information about a person’s
37 medical care) *and* autonomy privacy (because the potential for exposure of
38 stigmatizing private information could have a chilling effect on important choices
39 about medical care).

94. *Id.* at 35.

95. *Carey v. Population Services Int’l*, 431 U.S. 678, 684-85 (1977).

96. *Whalen v. Roe*, 429 U.S. 589 (1977).

1 On the facts before it, the Court was not persuaded:

2 Nor can it be said that any individual has been deprived of the right to decide
3 independently, with the advice of his physician, to acquire and to use needed
4 medication. Although the State no doubt could prohibit entirely the use of
5 particular Schedule II drugs, it has not done so. This case is therefore unlike
6 those in which the Court held that a total prohibition of certain conduct was an
7 impermissible deprivation of liberty. Nor does the State require access to these
8 drugs to be conditioned on the consent of any state official or other third party.
9 Within dosage limits which appellees do not challenge, the decision to prescribe,
10 or to use, is left entirely to the physician and the patient.

11 We hold that neither the immediate nor the threatened impact of the patient-
12 identification requirements in the New York State Controlled Substances Act of
13 1972 on either the reputation or the independence of patients for whom Schedule
14 II drugs are medically indicated is sufficient to constitute an invasion of any right
15 or liberty protected by the Fourteenth Amendment.⁹⁷

16 Moreover, an invasion of autonomy privacy of the type described above will
17 only arise if there has also been an invasion of informational privacy. If
18 informational privacy is protected, then any ancillary invasion of autonomy
19 privacy would also be avoided.

20 As discussed below, it is not entirely clear that the United States Constitution
21 protects informational privacy. In contrast, the California Constitution clearly does
22 provide such protection.

23 ***Informational Privacy***

24 It is not certain that a federal constitutional right of informational privacy exists.
25 There are cases that discuss such a right, but they do not clearly hold that the right
26 exists.

27 In *Whalen v. Roe* (discussed above),⁹⁸ the Court considered the constitutionality
28 of a state statute requiring that prescriptions for certain drugs be reported to law
29 enforcement. While the Court seemed to assume the existence of a constitutional
30 right of informational privacy, it did not expressly hold that such a right exists.
31 Nor did it articulate a standard for determining whether any constitutional right
32 had been violated.

33 However, the Court did recognize, in *dicta*, that government data collection
34 could, if conducted on a “massive” scale, implicate a duty to protect the privacy of
35 the collected information that “arguably has roots in the Constitution.”

36 We are not unaware of the threat to privacy implicit in the accumulation of vast
37 amounts of personal information in computerized data banks or other massive
38 government files. The collection of taxes, the distribution of welfare and social
39 security benefits, the supervision of public health, the direction of our Armed

97. *Id.* at 603-04 (footnotes omitted).

98. *Id.*

1 Forces, and the enforcement of the criminal laws all require the orderly
2 preservation of great quantities of information, much of which is personal in
3 character and potentially embarrassing or harmful if disclosed. The right to collect
4 and use such data for public purposes is typically accompanied by a concomitant
5 statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in
6 some circumstances that duty arguably has its roots in the Constitution,
7 nevertheless New York’s statutory scheme, and its implementing administrative
8 procedures, evidence a proper concern with, and protection of, the individual’s
9 interest in privacy. We therefore need not, and do not, decide any question which
10 might be presented by the unwarranted disclosure of accumulated private data —
11 whether intentional or unintentional — or by a system that did not contain
12 comparable security provisions. We simply hold that this record does not establish
13 an invasion of any right or liberty protected by the Fourteenth Amendment.⁹⁹

14 In *Nixon v. Administrator of General Services*,¹⁰⁰ the Court considered a statute
15 that required former President Richard Nixon to turn his presidential papers over
16 to government archivists for review (for the purpose of segregating public
17 documents, which would be archived, from private papers, which would be
18 returned to the President). President Nixon objected to the statutory obligation,
19 arguing in part that it would unconstitutionally invade his informational privacy.

20 The Court acknowledged that “[o]ne element of privacy has been characterized
21 as ‘the individual interest in avoiding disclosure of personal matters’”¹⁰¹ and found
22 that the President had a legitimate expectation of privacy with respect to some of
23 his papers. However, “the merit of appellant’s claim of invasion of his privacy
24 cannot be considered in the abstract; rather the claim must be considered in light
25 of the specific provisions of the Act, and any intrusion must be weighed against
26 the public interest in subjecting the presidential materials of appellant’s
27 administration to archival screening.”¹⁰² The court concluded that the statutory
28 procedures governing the screening and archiving of presidential papers were
29 sufficient to protect any privacy interest at issue (whatever its source).¹⁰³

30 Much more recently, in *National Aeronautics and Space Administration v.*
31 *Nelson*,¹⁰⁴ the Court considered whether certain pre-employment background
32 questionnaires violated a constitutional right of informational privacy. The Court
33 noted that most (but not all) circuit courts have found that there is a constitutional
34 right of informational privacy:

35 State and lower federal courts have offered a number of different interpretations
36 of *Whalen* and *Nixon* over the years. Many courts hold that disclosure of at least

99. *Id.* at 605-06 (footnote omitted).

100. 433 U.S. 425 (1977).

101. *Id.* at 457.

102. *Id.* at 458.

103. *Id.* at 465.

104. 562 U.S. 134 (2011).

1 some kinds of personal information should be subject to a test that balances the
2 government’s interests against the individual’s interest in avoiding disclosure.
3 *E.g.*, *Barry v. New York*, 712 F.2d 1554, 1559 (CA2 1983); *Fraternal Order of*
4 *Police v. Philadelphia*, 812 F.2d 105, 110 (CA3 1987); *Woodland v. Houston*,
5 940 F.2d 134, 138 (CA5 1991) (*per curiam*); *In re Crawford*, 194 F.3d 954, 959
6 (CA9 1999); *State v. Russo*, 259 Conn. 436, 459-464, 790 A.2d 1132, 1147-1150
7 (2002). The Sixth Circuit has held that the right to informational privacy protects
8 only intrusions upon interests “that can be deemed fundamental or implicit in the
9 concept of ordered liberty.” *J. P. v. DeSanti*, 653 F.2d 1080, 1090 (1981) (internal
10 quotation marks omitted). The D. C. Circuit has expressed “grave doubts” about
11 the existence of a constitutional right to informational privacy. *American*
12 *Federation of Govt. Employees v. HUD*, 118 F.3d 786, 791 (1997).¹⁰⁵

13 Nonetheless, the Court made clear that it was not deciding whether a
14 constitutional right of informational privacy exists. Instead, the Court *assumed* the
15 existence of a privacy interest of the type “mentioned” in *Whalen* and *Nixon*. It
16 then went on to explain why the statute at issue would not violate any
17 informational privacy interest that may “arguably” have its roots in the
18 Constitution:

19 In two cases decided more than 30 years ago, this Court referred broadly to a
20 constitutional privacy “interest in avoiding disclosure of personal matters.”
21 *Whalen v. Roe*, 429 U.S. 589, 599-600, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977);
22 *Nixon v. Administrator of General Services*, 433 U.S. 425, 457, 97 S. Ct. 2777, 53
23 L. Ed. 2d 867 (1977). ...

24 We assume, without deciding, that the Constitution protects a privacy right of
25 the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged
26 portions of the Government’s background check do not violate this right in the
27 present case. The Government’s interests as employer and proprietor in managing
28 its internal operations, combined with the protections against public dissemination
29 provided by the Privacy Act of 1974, 5 U.S.C. § 552a, satisfy any “interest in
30 avoiding disclosure” that may “arguably ha[ve] its roots in the Constitution.”
31 *Whalen, supra*, at 599, 605, 97 S. Ct. 869, 51 L. Ed. 2d 64.¹⁰⁶

32 Later in the opinion, the Court reemphasized that it was merely assuming the
33 existence of the informational privacy right. Moreover, it characterized *Whalen* as
34 having employed the same approach:

35 As was our approach in *Whalen*, we will assume for present purposes that the
36 Government’s challenged inquiries implicate a privacy interest of constitutional
37 significance.¹⁰⁷

38 To summarize, there is no United States Supreme Court precedent that clearly
39 recognizes a federal constitutional right of informational privacy. If such a right

105. *Id.* at 147 n. 9.

106. *Id.* at 138.

107. *Id.* at 147.

1 does exist, it is not clear what test the Court would apply to determine whether it
2 has been violated.

3 ***Informational Privacy and the Fourth Amendment***

4 Even if a constitutional right of informational privacy exists, it might not have
5 much relevance to the surveillance of electronic communications, because any
6 unenumerated right of informational privacy may be subsumed within the express
7 protections of the Fourth Amendment.

8 [T]he Government’s collection of private information is regulated by the Fourth
9 Amendment, and “[w]here a particular Amendment provides an explicit textual
10 source of constitutional protection against a particular sort of government
11 behavior, that Amendment, not the more generalized notion of substantive due
12 process, must be the guide for analyzing those claims.”¹⁰⁸

13 Concerns about the effect of electronic surveillance on privacy would seem to
14 fall squarely within the ambit of the Fourth Amendment. Under the principle
15 discussed above, one could argue that the “explicit textual source of constitutional
16 protection” provided in the Fourth Amendment should be used to test the
17 constitutionality of such searches, rather than a generalized notion of privacy
18 (whether grounded in substantive due process or in the penumbra of other
19 enumerated rights). If that is correct, then a federal constitutional right of
20 informational privacy would not be independently relevant in evaluating the
21 constitutionality of electronic surveillance.

22 ***Summary of Federal Constitutional Privacy Right***

23 There is a federal constitutional right of autonomy privacy. It protects the right
24 to make certain private decisions free from government interference. The cases
25 discussing autonomy privacy involve fundamentally private matters such as child-
26 rearing, procreation, marriage, and sexuality. Those types of concerns are unlikely
27 to have much direct relevance to electronic surveillance. To the extent that they
28 are indirectly relevant, that relevance would be a secondary effect of an invasion
29 of informational privacy.

30 It is not clear that there is a federal constitutional right of informational privacy.
31 The early cases on this issue seem to assume that such a right exists, but they do
32 not expressly hold that this is so. The more recent decision in *NASA v. Nelson* is
33 carefully framed to be noncommittal on the issue (and it claims that the same
34 noncommittal posture was employed in the earlier decisions).

108. *NASA v. Nelson*, 562 U.S. at 162 (Scalia, J., dissenting), quoting *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 rubric of substantive due process.”). See also *Graham v. Connor*, 490 U.S. 386, 395 (1989).

1 If such a right does exist, it does not appear to be absolute. In all of the cases
2 discussed above, the Court found that important governmental efforts to collect
3 data, with sufficient safeguards against improper disclosure of private information,
4 did not violate any constitutional right.

5 Moreover, there is precedent suggesting that any invasion of privacy falling
6 within the sphere of the Fourth Amendment must be analyzed under that
7 constitutional provision, rather than under a general liberty interest asserted as a
8 matter of substantive due process. The current study involves government
9 collection of information, which is susceptible to Fourth Amendment analysis. It is
10 thus unclear whether a privacy right grounded in substantive due process would
11 ever be applicable to the matters addressed in this study.

12 **Express Privacy Right in the California Constitution**

13 Unlike the United States Constitution, the California Constitution includes an
14 express right of privacy. Article I, Section 1 provides:

15 All people are by nature free and independent and have inalienable rights.
16 Among these are enjoying and defending life and liberty, acquiring, possessing,
17 and protecting property, and pursuing and obtaining safety, happiness, and
18 privacy.

19 That privacy right was added by initiative in 1972.¹⁰⁹

20 The first California Supreme Court case to construe the constitutional privacy
21 right was *White v. Davis*.¹¹⁰ That case concerned a Los Angeles Police Department
22 operation employing undercover officers who posed as college students in order to
23 attend class discussions and build dossiers on student activists and their professors.
24 Suit was filed to enjoin the practice. Among other grounds, the challengers alleged
25 that the police activities violated California's constitutional right of privacy.

26 The California Supreme Court found prima facie evidence that the program
27 violated constitutional rights of speech and assembly. It also found a prima facie
28 violation of the new privacy right:

29 [T]he surveillance alleged in the complaint also constitutes a prima facie
30 violation of the explicit "right of privacy" recently added to our state Constitution.
31 As we point out, a principal aim of the constitutional provision is to limit the
32 infringement upon personal privacy arising from the government's increasing
33 collection and retention of data relating to all facets of an individual's life. The
34 alleged accumulation in "police dossiers" of information gleaned from classroom
35 discussions or organization meetings presents one clear example of activity which
36 the constitutional amendment envisions as a threat to personal privacy and
37 security.¹¹¹

109. Prop. 11 (Nov. 7, 1972).

110. 13 Cal. 3d 757 (1975).

111. *Id.* at 761.

1 The Court held that the Constitution does not invalidate all information
2 gathering, but instead requires that the government show a “compelling
3 justification for such conduct.”¹¹²

4 In considering the effect of the new privacy right, the Court looked to the
5 election brochure materials for the proposition that created the right, stating that
6 such materials represent “in essence, the only ‘legislative history’ of the
7 constitutional amendment available to us.”¹¹³ The Court noted that it had “long
8 recognized the propriety of resorting to election brochure arguments as an aid in
9 construing legislative measures and constitutional amendments adopted pursuant
10 to a vote of the people.”¹¹⁴

11 The Court discussed the election brochure at some length:

12 In November 1972, the voters of California specifically amended article I,
13 section 1 of our state Constitution to include among the various “inalienable”
14 rights of “all people” the right of “privacy.” Although the general concept of
15 privacy relates, of course, to an enormously broad and diverse field of personal
16 action and belief, the moving force behind the new constitutional provision was a
17 more [focused] privacy concern, relating to the accelerating encroachment on
18 personal freedom and security caused by increased surveillance and data
19 collection activity in contemporary society. The new provision’s primary purpose
20 is to afford individuals some measure of protection against this most modern
21 threat to personal privacy.

22 The principal objectives of the newly adopted provision are set out in a
23 statement drafted by the proponents of the provision and included in the state’s
24 election brochure. The statement begins: “The proliferation of government
25 snooping and data collecting is threatening to destroy our traditional freedoms.
26 Government agencies seem to be competing to compile the most extensive sets of
27 dossiers of American citizens. Computerization of records makes it possible to
28 create “cradle-to-grave” profiles of every American. [para.] *At present there are
29 no effective restraints on the information activities of government and business.
30 This amendment creates a legal and enforceable right of privacy for every
31 Californian.*” (Italics in original.)

32 The argument in favor of the amendment then continues: “The right of privacy
33 is the right to be left alone. It is a fundamental and compelling interest. It protects
34 our homes, our families, our thoughts, our emotions, our expressions, our
35 personalities, our freedom of communion and our freedom to associate with the
36 people we choose. It prevents government and business interests from collecting
37 and stockpiling unnecessary information about us and from misusing information
38 gathered for one purpose in order to serve other purposes or to embarrass us.

39 *“Fundamental to our privacy is the ability to control circulation of personal
40 information.* [Italics in original.] This is essential to social relationships and
41 personal freedom. The proliferation of government and business records over
42 which we have no control limits our ability to control our personal lives. Often we

112. *Id.*

113. *Id.* at 775.

114. *Id.* at n. 11.

1 do not know that these records even exist and we are certainly unable to
2 determine who has access to them.

3 “Even more dangerous is the loss of control over the accuracy of government
4 and business records of individuals. Obviously if the person is unaware of the
5 record, he or she cannot review the file and correct inevitable mistakes. . . . [para.]
6 The average citizen . . . does not have control over what information is collected
7 about him. Much is secretly collected. . . .”

8 The argument concludes: “The right of privacy is an important American
9 heritage and essential to the fundamental rights guaranteed by the First, Third,
10 Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should
11 be abridged only when there is a compelling public need. . . .”¹¹⁵

12 Some important points can be drawn from that discussion:

- 13 • The focus on “government snooping and data collecting” are directly
14 germane to the propriety of electronic surveillance, which is specifically
15 noted as a concern. This is especially true given the modern capacity to
16 easily collect very large amounts of electronic data. For example, the
17 National Security Agency’s “Bulk Telephony Metadata Program” is
18 reported to have been collecting telephone dialing information from
19 virtually every phone in the country, for several years.¹¹⁶ Regardless of
20 whether such data collection is a “search” under the Fourth Amendment, it
21 seems to be the sort of “government snooping and data collecting” that
22 prompted the creation of California’s constitutional privacy right.
- 23 • The privacy right is “fundamental” and “compelling.” These are familiar
24 constitutional terms of art that imply a high level of dignity and protection.
- 25 • There is particular concern about data collection without notice. Such
26 secrecy makes it difficult for a person to “control circulation of personal
27 information” and to correct any errors in information the government has
28 gathered.

29 In another decision made later the same year, *Valley Bank of Nevada v. Superior*
30 *Court of San Joaquin County*,¹¹⁷ the Court considered a privacy-based objection to
31 a civil discovery order requiring the production of non-party bank records.

32 The Court found that the privacy right applies to confidential bank records:

33 Although the amendment is new and its scope as yet is neither carefully defined
34 nor analyzed by the courts, we may safely assume that the right of privacy
35 extends to one’s confidential financial affairs as well as to the details of one’s
36 personal life.¹¹⁸

37 Consequently, there must be a “careful balancing of the right of civil litigants to
38 discover relevant facts, on the one hand, with the right of bank customers to

115. *Id.* at 773-75 (footnotes omitted).

116. See *Klayman v. Obama*, 957 F. Supp. 2d 1, 14-20 (D.D.C. 2013).

117. 15 Cal. 3d 652 (1975).

118. *Id.* at 656.

1 maintain reasonable privacy regarding their financial affairs, on the other.”¹¹⁹
2 While private bank records “should not be wholly privileged and insulated from
3 scrutiny by civil litigants,” neither should they be disclosed without the subject of
4 the records having notice and an opportunity to object.¹²⁰ The Court put it this
5 way:

6 Striking a balance between the competing considerations, we conclude that
7 before confidential customer information may be disclosed in the course of civil
8 discovery proceedings, the bank must take reasonable steps to notify its customer
9 of the pendency and nature of the proceedings and to afford the customer a fair
10 opportunity to assert his interests by objecting to disclosure, by seeking an
11 appropriate protective order, or by instituting other legal proceedings to limit the
12 scope or nature of the matters sought to be discovered.¹²¹

13 *Private Action*

14 In *Hill v. National Collegiate Athletic Association*,¹²² the California Supreme
15 Court considered a constitutional privacy-based challenge to an NCAA drug
16 testing program for college athletes. Because the NCAA is a nongovernmental
17 association, the Court was required to consider whether the constitutional privacy
18 right applies to private action.

19 In addressing that question, the Court noted that the ballot arguments were
20 “replete with references to information-amassing practices of both ‘government’
21 and ‘business.’” The Court also referred to a string of court of appeal decisions
22 finding that the privacy right applies to private action. In light of those authorities,
23 the Court held that California’s constitutional right of privacy creates a right of
24 action against private as well as government entities.

25 Private action is not directly relevant to government surveillance of electronic
26 communications, but it could have some indirect relevance. In California, all
27 communication service providers are constitutionally obliged to protect their
28 customers’ privacy. The existence of that obligation may have an effect on
29 reasonable expectations of privacy.

30 *Elements of the Privacy Right*

31 In *Hill v. NCAA*, the California Supreme Court took the opportunity to conduct a
32 fairly thorough review of California’s constitutional privacy right and its
33 antecedents in the United States Constitution and the common law. After
34 discussing those foundations, the Court set out the elements of a cause of action
35 for a breach of privacy under Article I, Section 1 of the California Constitution:

119. *Id.* at 657.

120. *Id.* at 658.

121. *Id.*

122. 7 Cal. 4th 1 (1994).

- 1 (1) The identification of a specific legally protected privacy interest.
- 2 (2) A reasonable expectation of privacy on the part of the plaintiff.
- 3 (3) A “serious” invasion of the protected privacy interest.

4 Those elements are discussed further below.

5 *Legally Protected Privacy Interest.* In discussing the scope of legally protected
6 privacy interests sufficient to trigger constitutional protection, the Court first drew
7 a distinction between informational privacy and autonomy privacy. It then
8 observed that the constitutional privacy right was primarily aimed at protecting
9 informational privacy:

10 Informational privacy is the core value furthered by the Privacy Initiative.
11 (*White v. Davis, supra*, 13 Cal. 3d at p. 774.) A particular class of information is
12 private when well-established social norms recognize the need to maximize
13 individual control over its dissemination and use to prevent unjustified
14 embarrassment or indignity. Such norms create a threshold reasonable expectation
15 of privacy in the data at issue. As the ballot argument observes, the California
16 constitutional right of privacy “prevents government and business interests from
17 [1] collecting and stockpiling unnecessary information about us and from [2]
18 misusing information gathered for one purpose in order to serve other purposes or
19 to embarrass us.”¹²³

20 This clear statement that protection of informational privacy is a “core” value
21 furthered by the California Constitution is important because of the uncertainty
22 (discussed above) about whether the United States Constitution affords any
23 protection to informational privacy.

24 The Court recognized that the ballot arguments also expressed concern about the
25 types of intimate and personal decisions at issue in autonomy privacy. It pointed
26 out, however, that the ballot arguments “do not purport to create any unbridled
27 right of personal freedom of action that may be vindicated in lawsuits against
28 either government agencies or private persons or entities.”¹²⁴

29 The Court concludes by noting that legally protected privacy rights are derived
30 from social norms, which must themselves be grounded in sources of positive law:

31 Whether established social norms safeguard a particular type of information or
32 protect a specific personal decision from public or private intervention is to be
33 determined from the usual sources of positive law governing the right to privacy
34 — common law development, constitutional development, statutory enactment,
35 and the ballot arguments accompanying the Privacy Initiative.¹²⁵

123. *Id.* at 35-36.

124. *Id.* at 36.

125. *Id.*

1 *Reasonable Expectation of Privacy.* Even when a legally recognized privacy
2 interest exists, the reasonableness of the expectation of privacy may affect any
3 claim that the interest has been unconstitutionally invaded:

4 The extent of [a privacy] interest is not independent of the circumstances.”
5 (*Plante v. Gonzalez, supra*, 575 F.2d at p. 1135.) Even when a legally cognizable
6 privacy interest is present, other factors may affect a person’s reasonable
7 expectation of privacy. For example, advance notice of an impending action may
8 serve to “limit [an] intrusion upon personal dignity and security” that would
9 otherwise be regarded as serious. (*Ingersoll v. Palmer, supra*, 43 Cal.3d at p.
10 1346 [upholding the use of sobriety checkpoints].)

11 In addition, customs, practices, and physical settings surrounding particular
12 activities may create or inhibit reasonable expectations of privacy. (See, e.g.,
13 *Whalen, supra*, 429 U.S. at p. 602 [51 L.Ed.2d at p. 75] [reporting of drug
14 prescriptions to government was supported by established law and “not
15 meaningfully distinguishable from a host of other unpleasant invasions of privacy
16 that are associated with many facets of health care”]; *Fraternal Order of Police,*
17 *Lodge No. 5 v. City of Philadelphia* (3d Cir. 1987) 812 F.2d 105, 114 [no invasion
18 of privacy in requirement that applicants for promotion to special police unit
19 disclose medical and financial information in part because of applicant awareness
20 that such disclosure “has historically been required by those in similar
21 positions”].)

22 A “reasonable” expectation of privacy is an objective entitlement founded on
23 broadly based and widely accepted community norms. (See, e.g., Rest.2d Torts,
24 *supra*, § 652D, com. c [“The protection afforded to the plaintiff’s interest in his
25 privacy must be relative to the customs of the time and place, to the occupation of
26 the plaintiff and to the habits of his neighbors and fellow citizens.”]¹²⁶)

27 The Court also noted that advance voluntary consent can affect a person’s
28 reasonable expectation of privacy: “the presence or absence of opportunities to
29 consent voluntarily to activities impacting privacy interests obviously affects the
30 expectations of the participant.”¹²⁷

31 *Serious Invasion of Privacy.* Finally, the Court held that a constitutional privacy
32 claim must involve a “serious” violation of a legally protected privacy interest.
33 The Court’s discussion of this element is short:

34 No community could function if every intrusion into the realm of private action,
35 no matter how slight or trivial, gave rise to a cause of action for invasion of
36 privacy. “Complete privacy does not exist in this world except in a desert, and
37 anyone who is not a hermit must expect and endure the ordinary incidents of the
38 community life of which he is a part.” (Rest.2d Torts, *supra*, § 652D, com. c.)
39 Actionable invasions of privacy must be sufficiently serious in their nature, scope,
40 and actual or potential impact to constitute an egregious breach of the social

126. *Id.* at 36-37.

127. *Id.*

1 norms underlying the privacy right. Thus, the extent and gravity of the invasion is
2 an indispensable consideration in assessing an alleged invasion of privacy.¹²⁸

3 This might seem to set a fairly high bar for an actionable claim, with the right of
4 privacy only protecting against “an egregious breach of social norms.” However,
5 the Court quickly revisited the elements described in *Hill v. NCAA* and made clear
6 that they are not as strict as it might appear.

7 In *Loder v. City of Glendale*,¹²⁹ the Court explained that the elements “should
8 not be understood as establishing significant *new* requirements or hurdles that a
9 plaintiff must meet in order to demonstrate a violation of the right to privacy under
10 the state Constitution...”¹³⁰

11 Under such an interpretation, *Hill* would constitute a radical departure from *all*
12 of the earlier state constitutional decisions of this court cited and discussed in
13 *Hill*..., decisions that uniformly hold that when a challenged practice or conduct
14 intrudes upon a constitutionally protected privacy interest, the interests or
15 justifications supporting the challenged practice must be weighed or balanced
16 against the intrusion on privacy imposed by the practice.¹³¹

17 Instead, the elements laid out in *Hill* are merely “threshold elements” that serve
18 to “screen out claims that do not involve a significant intrusion on a privacy
19 interest protected by the state constitutional privacy protection.”¹³² The Court went
20 on to make clear that this threshold screening is actually fairly modest:

21 These elements do not eliminate the necessity for weighing and balancing the
22 justification for the conduct in question against the intrusion on privacy resulting
23 from the conduct in any case that raises a genuine, nontrivial invasion of a
24 protected privacy interest.¹³³

25 Regarding the requirement that an invasion of privacy be “serious” in order to
26 qualify for constitutional protection, the Court explained that the requirement sets
27 a low standard:

28 Although in discussing the “serious invasion of privacy interest” element, the
29 opinion in *Hill* states at one point that “[a]ctionable invasions of privacy must be
30 sufficiently serious in their nature, scope, and actual or potential impact to
31 constitute an egregious breach of the social norms underlying the privacy
32 right”..., the opinion’s application of the element makes it clear that this element
33 is intended simply to screen out intrusions on privacy that are *de minimis* or
34 insignificant.¹³⁴

128. *Id.* at 37.

129. 14 Cal. 4th 846 (1997).

130. *Id.* at 891 (emphasis in original).

131. *Id.* (emphasis in original).

132. *Id.* at 893.

133. *Id.*

134. *Id.* at 895 n.22.

1 **Standard of Review**

2 In *White v. Davis* the Court held that the government must demonstrate a
3 “compelling” public need in order to justify its invasion of the California
4 Constitution’s privacy right.¹³⁵ The Court quoted the part of the ballot brochure
5 asserting that “[t]he right of privacy ... should be abridged only when there is a
6 compelling public need.”¹³⁶

7 In *Hill v. NCAA*, however, the Court made clear that the decision in *White v.*
8 *Davis* was limited to the facts of that case:

9 *White* signifies only that some aspects of the state constitutional right to privacy
10 — those implicating obvious government action impacting freedom of expression
11 and association — are accompanied by a “compelling state interest” standard.¹³⁷

12 After reviewing a number of appellate decisions relating to the privacy right, the
13 Court found that the compelling state interest standard only applies in cases
14 involving particularly serious invasions of important privacy interests:

15 The particular context, i.e., the specific kind of privacy interest involved and
16 the nature and seriousness of the invasion and any countervailing interests,
17 remains the critical factor in the analysis. Where the case involves an obvious
18 invasion of an interest fundamental to personal autonomy, e.g., freedom from
19 involuntary sterilization or the freedom to pursue consensual familial
20 relationships, a “compelling interest” must be present to overcome the vital
21 privacy interest. If, in contrast, the privacy interest is less central, or in bona fide
22 dispute, general balancing tests are employed.

23 For the reasons stated above, we decline to hold that every assertion of a
24 privacy interest under article I, section 1 must be overcome by a “compelling
25 interest.” Neither the language nor history of the Privacy Initiative unambiguously
26 supports such a standard. In view of the far-reaching and multifaceted character of
27 the right to privacy, such a standard imports an impermissible inflexibility into the
28 process of constitutional adjudication.¹³⁸

29 In other circumstances, a court need only consider whether an invasion of a
30 legally protected privacy interest is justified by a “legitimate” and “important”
31 competing interest:

32 Invasion of a privacy interest is not a violation of the state constitutional right
33 to privacy if the invasion is justified by a competing interest. Legitimate interests
34 derive from the legally authorized and socially beneficial activities of government
35 and private entities. Their relative importance is determined by their proximity to
36 the central functions of a particular public or private enterprise. Conduct alleged
37 to be an invasion of privacy is to be evaluated based on the extent to which it
38 furthers legitimate and important competing interests.

135. *White v. Davis*, 13 Cal. 3d at 776.

136. *Id.* at 775.

137. *Hill*, 7 Cal. 4th at 34.

138. *Id.* at 34-35 (footnote omitted).

1 Confronted with a defense based on countervailing interests, the plaintiff may
2 undertake the burden of demonstrating the availability and use of protective
3 measures, safeguards, and alternatives to defendant’s conduct that would
4 minimize the intrusion on privacy interests.¹³⁹

5 Importantly, the Court in *Hill* held that the standard of review may differ
6 depending on whether a privacy claim is brought against a public or private actor:

7 Judicial assessment of the relative strength and importance of privacy norms
8 and countervailing interests may differ in cases of private, as opposed to
9 government, action.

10 *First*, the pervasive presence of coercive government power in basic areas of
11 human life typically poses greater dangers to the freedoms of the citizenry than
12 actions by private persons. “The government not only has the ability to affect
13 more than a limited sector of the populace through its actions, it has both
14 economic power, in the form of taxes, grants, and control over social welfare
15 programs, and physical power, through law enforcement agencies, which are
16 capable of coercion far beyond that of the most powerful private actors.” (Sundby,
17 *Is Abandoning State Action Asking Too Much of the Constitution?* (1989) 17
18 Hastings Const. L. Q. 139, 142-143 [hereafter Sundby].)

19 *Second*, “an individual generally has greater choice and alternatives in dealing
20 with private actors than when dealing with the government.” (Sundby, *supra*, 17
21 Hastings Const.L.Q. at p. 143.) Initially, individuals usually have a range of
22 choice among landlords, employers, vendors and others with whom they deal. To
23 be sure, varying degrees of competition in the marketplace may broaden or
24 narrow the range. But even in cases of limited or no competition, individuals and
25 groups may turn to the Legislature to seek a statutory remedy against a specific
26 business practice regarded as undesirable. State and federal governments routinely
27 engage in extensive regulation of all aspects of business. Neither our Legislature
28 nor Congress has been unresponsive to concerns based on activities of
29 nongovernment entities that are perceived to affect the right of privacy. (See, e.g.,
30 Lab. Code, § 432.2, subd. (a) [“No employer shall demand or require any
31 applicant for employment or prospective employment or any employee to submit
32 to or take a polygraph, lie detector or similar test or examination as a condition of
33 employment or continued employment”]; 29 U.S.C. § 2001 [regulating private
34 employer use of polygraph examination].)

35 *Third*, private conduct, particularly the activities of voluntary associations of
36 persons, carries its own mantle of constitutional protection in the form of freedom
37 of association. Private citizens have a right, not secured to government, to
38 communicate and associate with one another on mutually negotiated terms and
39 conditions. The ballot argument recognizes that state constitutional privacy
40 protects in part “our freedom of communion and our freedom to associate with the
41 people we choose.” (Ballot Argument, *supra*, at p. 27.) Freedom of association is
42 also protected by the First Amendment and extends to all legitimate organizations,
43 whether popular or unpopular. (*Britt v. Superior Court* (1978) 20 Cal. 3d 844, 854
44 [143 Cal. Rptr. 695, 574 P.2d 766]; see also Tribe, *American Constitutional Law*
45 (2d ed. 1988) § 18-2, p. 1691 [noting rationale of federal constitutional

139. *Id* at 38.

1 requirement of state action protects “the freedom to make certain choices, such as
2 choices of the persons with whom [one associates]” which is “basic under any
3 conception of liberty”).¹⁴⁰

4 The *Hill* argument focuses on explaining why a lower standard might be
5 appropriate when reviewing the action of private groups. Yet it also contains a
6 strong inference that the converse is true as well. When the *government* invades a
7 privacy interest, the standard of review should arguably be stricter than when a
8 private party engages in similar behavior.

9 For example, this report examines government surveillance of electronic
10 communications. In that context, the government is acting with the full coercive
11 power of the state, there are no choices that a citizen could make to avoid the
12 government’s actions, and the government deserves no special consideration that
13 might be due to protect the association rights of private voluntary groups. Thus,
14 none of the rationales offered in the passage quoted above would seem to justify
15 applying a lower standard when reviewing electronic surveillance.

16 ***Informational Privacy and Article I, Section 13 of the California Constitution***

17 As discussed above, any unenumerated federal constitutional right of
18 informational privacy may be subsumed within the express protections of the
19 Fourth Amendment.¹⁴¹ A similar principle has been applied to California’s express
20 privacy right, with regard to cases that involve a government search and seizure.

21 In *People v. Crowson*,¹⁴² two men were arrested and placed into the back of a
22 locked police car. While left alone in the vehicle, the two conversed. Their
23 conversation was secretly recorded and the recording was introduced as evidence
24 at trial. Mr. Crowson challenged the recording on the grounds that police had
25 violated his right to privacy under Article I, Section 1 of the California
26 Constitution.

27 The Court found that there had been no violation of the constitutional privacy
28 right, because the defendant had no “reasonable expectation of privacy” under the
29 circumstances. The Court expressly applied the same test that is used to determine
30 whether there has been a “search” under the Fourth Amendment of the United
31 States Constitution, or Article I, Section 13 of the California Constitution. It
32 explained:

33 In the search and seizure context, the article I, section 1 “privacy” clause has
34 never been held to establish a broader protection than that provided by the Fourth
35 Amendment of the United States Constitution or article I, section 13 of the
36 California Constitution. “[The] search and seizure and privacy protections [are]
37 coextensive when applied to police surveillance in the criminal context.” (*People*
38 *v. Owens* (1980) 112 Cal.App.3d 441, 448-449 [169 Cal. Rptr. 359].) “[Article I,

140. *Id.* at 38-39.

141. See *supra* notes 24-26 & accompanying text.

142. 33 Cal. 3d 623 (1983).

1 section 1, article I, section 13 and the Fourth Amendment] apply only where
2 parties to the [conversation] have a ‘reasonable expectation of privacy’ with
3 respect to what is said....” (*People v. Estrada* (1979) 93 Cal.App.3d 76, 98 [155
4 Cal. Rptr. 731].)¹⁴³

5 The defendant argued that *White v. Davis* had established stronger protections
6 for the constitutional privacy right. The Court responded:

7 Crowson argues that in *White v. Davis* ... we held that article I, section 1
8 establishes an expanded right of privacy which may be abridged only where there
9 is a compelling state interest. *White*, however, was not a traditional search and
10 seizure case, but rather involved alleged police surveillance of noncriminal
11 activity on a university campus. In that context, we held that the alleged police
12 conduct implicated First Amendment as well as right to privacy principles.¹⁴⁴

13 The holding and reasoning in *Crowson* suggest that any case involving a
14 “traditional search and seizure” should be analyzed under the Fourth Amendment
15 and Article I, Section 13 of the California Constitution, rather than under the
16 Article I, Section 1 privacy right.

17 The California Supreme Court made that point expressly in *In re York*,¹⁴⁵ in
18 which petitioners objected to a rule requiring drug testing as a condition of
19 releasing a criminal suspect on the suspect’s own recognizance pending trial. The
20 practice was claimed to violate the suspect’s Article I, Section 1 right to privacy,
21 as well as constitutional protections against unreasonable search and seizure under
22 the Fourth Amendment and Article I, Section 13. The Court set aside the privacy
23 claim, and analyzed the case solely under search and seizure principles, in express
24 reliance on *Crowson*:

25 We also observe that, “[i]n the search and seizure context, the article I, section
26 1 ‘privacy’ clause [of the California Constitution] has never been held to establish
27 a broader protection than that provided by the Fourth Amendment of the United
28 States Constitution or article I, section 13 of the California Constitution.” (*People*
29 *v. Crowson* (1983) 33 Cal.3d 623, 629 [190 Cal. Rptr. 165, 660 P.2d 389].)¹⁴⁶

30 ***Summary of California Constitutional Privacy Right***

31 The California Constitution contains an express privacy right. That right applies
32 to both public and private action. The privacy right protects both informational
33 privacy and autonomy privacy.

34 In order to “weed out” trivial, insignificant, and de minimis privacy violations,
35 courts first determine whether a privacy right claim meets the following threshold

143. *Id.* at 629.

144. *Id.* at n.5.

145. 9 Cal. 4th 1133 (1995).

146. *Id.* at 1149.

1 elements: (1) an identifiable privacy interest, (2) a reasonable expectation of
2 privacy, and (3) a serious violation of the privacy interest.

3 If an actionable claim is presented, the invasion of privacy may be justified by
4 demonstrating a legitimate and important competing interest. This requires a
5 balancing analysis, which takes into account the kind of privacy interest involved,
6 the nature and seriousness of the invasion, and the nature of the countervailing
7 interests. The level of protection may be lower when private party action is at
8 issue. This implies that the converse may also be true, that stricter standards apply
9 when reviewing government action.

10 In cases involving a traditional search and seizure (e.g., “police surveillance in
11 the criminal context”), the protection afforded by the privacy right is no greater
12 than that afforded by the Fourth Amendment or Article I, Section 13 of the
13 California Constitution.

14 FEDERAL SURVEILLANCE STATUTES

15 In addition to complying with federal and state constitutional constraints, state
16 legislation on government access to electronic communications must comply with
17 any controlling federal statutory law. In that regard, it is important to examine and
18 consider the requirements of the Electronic Communications Privacy Act of 1986
19 (“ECPA”). ECPA is a federal bill, enacted in 1986, which modernized federal
20 statutory law governing electronic surveillance.¹⁴⁷ The official name of the bill is
21 commonly used as a shorthand, to refer to the statutes that were amended or added
22 by the bill. For the purposes of this study, the most relevant effects of ECPA are as
23 follows:

- 24 • ECPA amended an existing statute on the interception of wire and oral
25 communications (Chapter 119 of Title 18, also known as the “Wiretap Act”
26 or “Title III”) to make that statute applicable to electronic communications.
- 27 • ECPA added a new statute on access to stored electronic communications
28 (Chapter 121 of Title 18, also known as the “Stored Communications Act”
29 or “SCA”).
- 30 • ECPA added a new statute on the use of pen registers and trap and trace
31 devices (Chapter 206 of Title 18, hereafter “Pen Register Act”).

32 ECPA is relevant to the conduct of electronic surveillance in California for two
33 reasons: It expressly applies to the states and it has been held to preempt less
34 protective state laws.¹⁴⁸ Federal preemption is a consequence of the “Supremacy
35 Clause” of the United States Constitution.¹⁴⁹

147. P.L. 99-508; 100 Stat. 1848 (1986)

148. See *Florida Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132 (1963) (federal preemption doctrine generally); *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 105-06 (2006) (federal Wiretap Act does not preempt more stringent protections of California law); *People v. Conklin*, 12 Cal. 3d 259 (1974) (“[T]he Senate Report indicates that Congress anticipated state regulation of electronic

1 interception for the purposes of the Wiretap Act. Instead, it is regulated under the
2 Stored Communications Act, which is discussed later in this report.

3 However, it is possible to “intercept” an electronic communication during
4 transmission, and such interceptions are governed by the Wiretap Act. The fact
5 that the process of sending an electronic communication necessarily creates a
6 stored copy of the communication does not bar application of the Wiretap Act:

7 The term “electronic communication” includes transient electronic storage
8 intrinsic to the transmission of such communications. Thus, an e-mail message
9 continued to be an electronic communication during momentary intervals,
10 intrinsic to the communication process, when the message is in transient
11 electronic storage. Interception of electronic communication occurs with reading
12 of transmissions as they are sent....¹⁵⁴

13 **Prohibitions and Exceptions**

14 It is generally unlawful to intentionally intercept a wire, oral, or electronic
15 communication.¹⁵⁵ It is also generally unlawful to disclose or use the contents¹⁵⁶ of
16 communications that are known to have been obtained through an unlawful
17 interception or that are disclosed in order to obstruct a criminal investigation.¹⁵⁷ In
18 addition, electronic communication service providers are generally prohibited
19 from divulging the contents of communications, while they are in transmission, to
20 anyone other than the sender or intended recipient.¹⁵⁸ Finally, it is unlawful to
21 manufacture, sell, advertise, or deliver devices designed for surreptitious
22 interception of wire, oral, or electronic communications.¹⁵⁹

23 Those general prohibitions are subject to a number of exceptions. Many of the
24 exceptions relate to matters that are not germane to state and local agency
25 surveillance, such as exceptions for the interception of publicly accessible
26 information,¹⁶⁰ interception with the consent of a participant,¹⁶¹ and interception
27 pursuant to the legitimate business needs of the service provider.¹⁶² There are also

154. J. Carr & P. Bellia, *The Law of Electronic Surveillance*, 3:7 (Feb. 2014) (footnotes omitted) (hereafter “*Electronic Surveillance*”).

155. 18 U.S.C. § 2511(1)(a)-(b).

156. In Chapter 119, “contents” is a defined term. See 18 U.S.C. § 2510(8) (“‘contents’, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication...”).

157. 18 U.S.C. § 2511(1)(c)-(e).

158. 18 U.S.C. § 2511(3)(a).

159. 18 U.S.C. § 2512(1).

160. 18 U.S.C. § 2512(2)(g).

161. 18 U.S.C. § 2512(2)(c)-(d), (3)(b)(ii).

162. 18 U.S.C. § 2512(2)(a)(i)-(ii); (3)(b)(iii).

1 exceptions for interception for specified federal purposes.¹⁶³ Federal interception is
2 beyond the scope of this report.

3 **Government Interception Pursuant to Warrant**

4 Notwithstanding the general prohibitions of the Wiretap Act, government may
5 intercept wire, oral, and electronic communications pursuant to a lawfully issued
6 warrant.¹⁶⁴

7 As discussed earlier, a warrant authorizing the interception of communications
8 is subject to stricter requirements than a routine search warrant. This reflects the
9 special Fourth Amendment concerns that arise when government intercepts
10 communications.¹⁶⁵ The main requirements for issuance of the so-called “super-
11 warrant” are as follows:

- 12 • Interception can only be authorized to investigate specified serious
13 felonies.¹⁶⁶
- 14 • The court must find that other investigative procedures were tried and failed,
15 were unlikely to succeed if tried, or would be too dangerous to try.¹⁶⁷
- 16 • Authorization to intercept communications may not continue “longer than is
17 necessary to achieve the objective of the authorization, nor in any event
18 longer than thirty days.”¹⁶⁸ However, based on a new showing of probable
19 cause, the court can extend the authorization for one or more additional
20 periods of the same duration.¹⁶⁹
- 21 • The interception must be “conducted in such a way as to minimize the
22 interception of communications not otherwise subject to interception” under
23 the Wiretap Act.¹⁷⁰
- 24 • The warrant must describe the person whose communications will be
25 intercepted (if known), the communication facilities to be used, the type of
26 communication to be intercepted and the criminal offense to which it
27 relates.¹⁷¹

163. 18 U.S.C. § 2512(2)(b) (Federal Communications Commission); (2)(e)-(f) (foreign intelligence gathering).

164. 18 U.S.C. § 2517. There are also specific exceptions for the disclosure of intercepted content to law enforcement, in situations other than government surveillance. See 18 U.S.C. § 2511(2)(i) (computer trespasser), (3)(b)(iv) (inadvertently obtained evidence of crime).

165. See text accompanying notes 42-44 (discussing *New York v. Berger*).

166. 18 U.S.C. § 2516(1) (federal government), (2) (state government). The standard is lower when the federal government intercepts electronic communications in the former situation than when a state government intercepts electronic communications. Any federal felony is sufficient. *Id.* at (3).

167. 18 U.S.C. § 2518(3)(c).

168. 18 U.S.C. § 2518(5).

169. *Id.*

170. *Id.*

171. 18 U.S.C. § 2518(4).

- 1 • In addition to finding probable cause for belief that an individual is
2 committing, has committed, or is about to commit a predicate crime, the
3 court must also find “probable cause for belief that particular
4 communications concerning that offense will be obtained through such
5 interception” and “probable cause for belief that the facilities from which, or
6 the place where, the wire, oral, or electronic communications are to be
7 intercepted are being used, or are about to be used, in connection with the
8 commission of such offense, or are leased to, listed in the name of, or
9 commonly used by such person.”¹⁷²
- 10 • The contents of intercepted communications are required to be recorded in
11 a form that will prevent alteration. On expiration of the period of
12 authorization, the recordings must be made available to the judge.¹⁷³
- 13 • Within a reasonable time (not to exceed 90 days) after an authorizing order
14 and any extension of the order has terminated, an “inventory” shall be
15 served on the persons named in the order and on any other party to an
16 intercepted communication as the judge orders, in the interests of justice.
17 The inventory document must provide notice of the interception, including
18 the date and period of interception, and whether any communications were
19 actually intercepted. The judge may also order, in the interests of justice,
20 that portions of the intercepted communications be provided. However, on
21 an ex parte showing of good cause, a judge may postpone service of the
22 inventory.¹⁷⁴

23 **Exception to Warrant Requirement for Exigent Circumstances**

24 In certain circumstances, law enforcement may intercept a wire, oral, or
25 electronic communication without first obtaining an authorizing court order. This
26 may be done if (1) law enforcement determines that there is an emergency that
27 requires the interception to occur before an order could be obtained with due
28 diligence, (2) there are grounds upon which an authorizing order could be entered,
29 and (3) an application for an authorizing order is made within 48 hours after the
30 interception begins.¹⁷⁵

31 For this purpose, an emergency situation must involve one or more of the
32 following:

- 33 • Immediate danger of death or serious physical injury to any person.
- 34 • Conspiratorial activities threatening the national security interest.
- 35 • Conspiratorial activities characteristic of organized crime.¹⁷⁶

172. 18 U.S.C. § 2518(3).

173. 18 U.S.C. § 2518(8)(a).

174. 18 U.S.C. § 2518 (8)(d).

175. 18 U.S.C. § 2518(7).

176. *Id.*

1 An interception conducted pursuant to this emergency exception must end
2 immediately when the communication being sought has been obtained or the court
3 denies the requested order, whichever comes first.¹⁷⁷

4 If the court denies the application for authority, or the application is never made,
5 the interception is treated as a violation of the chapter.¹⁷⁸

6 **Use of Lawfully Intercepted Communications**

7 An investigative or law enforcement officer who lawfully obtains the contents of
8 an interception of a wire, oral, or electronic communication can disclose those
9 contents to another investigative or law enforcement officer to the extent
10 appropriate to the proper performance of official duties.¹⁷⁹ Such contents can also
11 be used by the investigative or law enforcement officer in the proper performance
12 of official duties.¹⁸⁰ The same is true even if the officer intercepts communications
13 relating to offenses other than those specified in the order authorizing
14 interception.¹⁸¹

15 Any person who lawfully received the contents of an intercepted communication
16 or evidence derived from the interception may disclose the contents or derivative
17 evidence while giving testimony under oath or affirmation in any proceeding
18 under the authority of the federal government, a state, or a political subdivision of
19 a state.¹⁸² However, if an officer intercepts communications relating to offenses
20 other than those specified in the order authorizing interception, the contents of the
21 interception and derivative evidence can only be introduced into evidence in a
22 proceeding if a judge determines, on subsequent application, that the contents
23 were otherwise intercepted in accordance with the Wiretap Act.¹⁸³

24 There are also provisions authorizing use of lawfully intercepted communication
25 contents in foreign intelligence, counter-intelligence, and foreign intelligence
26 sharing, and to counter a grave threat from foreign powers, saboteurs, terrorists, or
27 foreign intelligence agents.¹⁸⁴ Such use is beyond the scope of this report.

28 **Limitations on Use of Intercepted Communications**

29 The contents of a lawfully intercepted communication cannot be introduced into
30 evidence in a proceeding unless all parties receive a copy of the application, as
31 well as the order authorizing the interception, at least 10 days before the

177. *Id.*

178. *Id.*

179. 18 U.S.C. § 2517(1).

180. 18 U.S.C. § 2517(2).

181. 18 U.S.C. § 2517(5).

182. 18 U.S.C. § 2517(3).

183. 18 U.S.C. § 2517(5).

184. 18 U.S.C. § 2517(6)-(8).

1 proceeding.¹⁸⁵ The judge may waive the 10-day period if it was not possible to
2 provide notice to a party in that time period and the party was not prejudiced.¹⁸⁶

3 A privileged communication does not lose its privileged status as a consequence
4 of being lawfully intercepted.¹⁸⁷

5 **Remedies for Violations**

6 The remedies provided in the Wiretap Act are the exclusive remedies for a
7 violation of that act. However, this does not limit the remedies that might be
8 available if a statutory violation also violates the Constitution.¹⁸⁸

9 The act provides for the following types of relief:

- 10 • *Injunction.* The United States Attorney General may bring an action to
11 enjoin a felony violation of the Wiretap Act.¹⁸⁹
- 12 • *Suppression of Evidence.* Before any “trial, hearing, or proceeding in or
13 before any court, department, officer, agency, regulatory body, or other
14 authority of the United States, a State, or a political subdivision thereof,” an
15 “aggrieved person”¹⁹⁰ may move to suppress the contents of an interception
16 or evidence derived from those contents.¹⁹¹
- 17 • *Civil Action Generally.* In general, a person whose communication is
18 intercepted, disclosed, or intentionally used in violation of the Wiretap Act,
19 by a person other than the United States, may bring a civil action seeking
20 preliminary or declaratory relief, damages, fees, and costs.
- 21 • *Civil Action Against United States.* Any person who is aggrieved by a
22 willful violation of the Wiretap Act by the United States may bring a civil
23 action against the United States for money damages.¹⁹²
- 24 • *Administrative Discipline.* An officer of the United States who willfully or
25 intentionally violates the chapter may be subject to administrative
26 discipline.¹⁹³
- 27 • *Criminal Penalty.* A person who violates the general prohibitions in the
28 Wiretap Act may be punished by a fine, imprisoned for not more than five
29 years, or both.¹⁹⁴

185. 18 U.S.C. § 2518(9).

186. *Id.*

187. 18 U.S.C. § 2517(4).

188. 18 U.S.C. § 2518(10)(c).

189. 18 U.S.C. § 2521.

190. 18 U.S.C. § 2510(11) (“‘aggrieved person’ means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed...”).

191. 18 U.S.C. § 2518(10)(a).

192. 18 U.S.C. § 2712(a).

193. 18 U.S.C. § 2520(f). See also 18 U.S.C. § 2712(c).

194. 18 U.S.C. § 2511(4)(a).

- 1 • *Contempt.* A violation of certain procedures governing law enforcement
2 interception pursuant to court authorization is punishable as contempt.¹⁹⁵
- 3 • *Confiscation of Devices.* Devices that are used, sent, carried, manufactured,
4 assembled, possessed, sold or advertised in violation of the relevant
5 provisions of the Wiretap Act can be seized and forfeited to the United
6 States.¹⁹⁶

7 A person has a complete defense to civil and criminal liability under the Wiretap
8 Act if the person acted in good faith reliance on a court order or warrant, an
9 emergency request, or a good faith determination that the law permitted the
10 conduct that is alleged to be a violation of the act.¹⁹⁷

11 Access to Stored Communications

12 The Stored Communications Act, an important component of ECPA, governs
13 the disclosure of stored electronic communications, including both content and
14 metadata. Access to and disclosure of such information is generally prohibited,
15 unless it falls within a statutory exception. There are a series of exceptions for
16 government access pursuant to lawful process (with the type of process required
17 varying with the type of information sought). The major elements of the statute are
18 described below.

19 **Prohibitions and Exceptions**

20 It is generally unlawful to do any of the following:

- 21 • Intentionally access an electronic communication service¹⁹⁸ facility, without
22 authorization or in excess of authorization, to obtain, alter, or prevent
23 authorized access to a wire or electronic communication that is in electronic
24 storage.¹⁹⁹
- 25 • For an electronic communication service provider to knowingly divulge, to
26 any person or entity, the contents of a communication that is in electronic
27 storage.²⁰⁰
- 28 • For a remote computing service²⁰¹ provider to knowingly divulge, to any
29 person or entity, the contents of any communication that is “carried or

195. 18 U.S.C. § 2518(8)(c).

196. 18 U.S.C. § 2513.

197. 18 U.S.C. § 2520(d).

198. See 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.”). See also 18 U.S.C. § 2711(1) (expressly making definitions in Section 2510 applicable to Chapter 121).

199. 18 U.S.C. § 2701(a).

200. 18 U.S.C. § 2702(a)(1).

201. 18 U.S.C. § 2711(2) (“remote computing service” is defined as “the provision to the public of computer storage or processing services by means of an electronic communications system ...”).

1 maintained” on the remote computing service on behalf of a customer or
2 subscriber.²⁰²

- 3 • For an electronic communication service provider or a remote computing
4 service provider to knowingly divulge, to any person or entity, a record or
5 other information pertaining to a customer or subscriber.²⁰³

6 Furthermore, any willful disclosure of a record lawfully obtained by law
7 enforcement pursuant to the Stored Communications Act is deemed to be a
8 violation of the Act, unless (1) the disclosure was made in the proper performance
9 of official functions or (2) the disclosed information had previously been lawfully
10 disclosed by the government or by the plaintiff in a civil action relating to the
11 disclosure.²⁰⁴

12 Those general prohibitions are subject to a number of exceptions. Many of the
13 exceptions relate to matters that are not germane to government surveillance, such
14 as exceptions for disclosure of intercepted information with the consent of a
15 communication participant,²⁰⁵ disclosure pursuant to the legitimate business needs
16 of the service provider,²⁰⁶ and disclosure to federal intelligence agencies.²⁰⁷

17 **Government Interception Pursuant to Lawful Process**

18 There are a number of exceptions for government access to stored data. In each
19 of these exceptions, a provider is compelled to provide information when a
20 government entity presents the requisite authorization. The form of authorization
21 required varies, based on the following factors:

- 22 • Whether the information sought is held in connection with an “electronic
23 communication service” (hereafter “ECS”) or a “remote computing service”
24 (hereafter “RCS”).
- 25 • If the information is held in connection with an RCS service, whether that
26 service is provided to the general public.
- 27 • Whether the information is content or metadata.
- 28 • Whether the information has been stored for 180 days or more.

29 Those distinctions, and the system of requirements based on those distinctions,
30 are discussed further below.

202. 18 U.S.C. § 2702(a)(2).

203. 18 U.S.C. § 2702(a)(3).

204. 18 U.S.C. § 2707(g).

205. 18 U.S.C. §§ 2701(c)(2); 2702(b)(1) & (3), (c)(2).

206. 18 U.S.C. § 2702(b)(4)-(5), (c)(3).

207. 18 U.S.C. § 2709.

1 ***ECS v. RCS***

2 In very general terms, an ECS is a system used to send and receive
3 communications on behalf of a customer (e.g., an email service), while an RCS is
4 a system used to store or process customer data (e.g., an online cloud storage
5 service).

6 One potential difficulty with the ECS-RCS dichotomy is that the delivery and
7 receipt of electronic communications also involves the creation and storage of
8 copies. To partially resolve that difficulty, the Stored Communications Act
9 provides that ECS can include a copy of a message that is in “electronic
10 storage.”²⁰⁸ That term is defined narrowly:

11 (17) “electronic storage” means—

12 (A) any temporary, intermediate storage of a wire or electronic communication
13 incidental to the electronic transmission thereof; and

14 (B) any storage of such communication by an electronic communication service
15 for purposes of backup protection of such communication

16 Any stored communication that does not fall within the above definition of
17 “electronic storage” would instead be deemed to be in the kind of storage provided
18 by an RCS.

19 Applying those concepts, some courts have held that an email message remains
20 in “electronic storage” (i.e., within ECS status) only until it has been opened. Once
21 the message has been opened, any further storage is no longer “temporary” or
22 “incidental to ... transmission.” At that point, any further storage of the opened
23 message is the sort of storage provided by an RCS.²⁰⁹

24 However, there is a split of authority on that issue. In *Theofel v. Farey-Jones*,
25 the court held that a copy of an opened email had been retained by the ISP as a
26 “backup.” Consequently, the message was in “electronic storage” under the
27 backup clause in the governing definition. Thus, access to the opened email was
28 governed by the provisions that apply to an ECS service.²¹⁰

29 ***RCS Service to the “Public”***

30 The definition of “remote computing service” is limited to an entity that
31 provides service to the “public.” This includes any entity that offers services to the
32 public generally (e.g., Gmail).

33 It does not include an entity that provides service solely on the basis of a special
34 relationship between the entity and the users of the service. For example, a
35 company that provides email service to its employees as an incident of

208. See, e.g., 18 U.S.C. § 2702(a) (prohibiting ECS disclosure of message content “while in electronic storage by that service”).

209. Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 120 (2009) (and cases cited therein).

210. 359 F.3d 1066, 1075-77 (9th Cir. 2004).

1 employment would not be providing service to the “public” and so would not be
2 an RCS with regard to its employees.²¹¹

3 Some commentators have expressed concern that the definition of “RCS” may
4 exclude universities that provide Internet services to their students, because those
5 services are not being provided to the public generally.²¹² If so, the privacy
6 protections afforded to RCS data could be denied to those who receive Internet
7 service from a university or similar entity.

8 ***Content and Metadata***

9 The Stored Communications Act draws an express distinction between the
10 content of a communication and related non-content information.²¹³

11 The SCA also draws a distinction between non-content information generally²¹⁴
12 and a specific subset of non-content information (identifying the customer and
13 detailing the customer’s telephone use).²¹⁵

14 **Required Legal Process**

15 Depending on the circumstances, the Stored Communications Act may require a
16 warrant, a grand jury subpoena, an administrative subpoena, or a court order
17 issued under 18 U.S.C. § 2703(d) when government seeks to compel the
18 production of stored communications.

19 The forms of legal process that government must use to access different types of
20 information are summarized in the table below:

Information Sought	Required Process
ECS Content Stored 180 Days or Less	• Search warrant ²¹⁶
ECS Content Stored More Than 180 Days	• Search warrant, ²¹⁷ or • Administrative subpoena, or • Grand jury or trial subpoena, or • Court order per § 2703(d) ²¹⁸
RCS Content	• Search warrant, ²¹⁹ or • Administrative subpoena, or

211. Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 119-20 (2009).

212. Kerr, *A User’s Guide to the Stored Communications Act – and a Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev. 1, 22 (2004).

213. See generally 18 U.S.C. § 2703.

214. 18 U.S.C. § 2703(c)(1).

215. 18 U.S.C. § 2703(c)(2).

216. 18 U.S.C. § 2703(a).

217. 18 U.S.C. § 2703(a) & (b)(1)(A).

218. 18 U.S.C. § 2703(b)(1)(B)(i).

219. 18 U.S.C. § 2703(a) & (b)(1)(A).

	<ul style="list-style-type: none">• Grand jury or trial subpoena, or• Court order per § 2703(d)²²⁰
Non-Content Information Generally	<ul style="list-style-type: none">• Search warrant,²²¹ or• Court order per § 2703(d)²²²
Specified Subset of Non-Content Information (“Subscriber Information”)	<ul style="list-style-type: none">• Search warrant,²²³ or• Administrative subpoena, or• Grand jury or trial subpoena, or• Court order per § 2703(d)²²⁴
RCS that is not Provided to the Public Generally	<ul style="list-style-type: none">• No protection under the SCA

1 In addition, the Stored Communications Act provides an exception for the
2 disclosure of stored communications to address an emergency²²⁵ and
3 miscellaneous other exceptions relating to specific law enforcement situations.²²⁶

4 **Noteworthy Implications of Existing Statutory Rules**

5 A few aspects of the legal process requirements described above warrant further
6 discussion.

7 ***Possible Unconstitutionality of Section 2703(d) Order***

8 As noted above, the Stored Communications Act sometimes authorizes the use
9 of a court order issued under Section 2703(d) to compel the production of stored
10 electronic records. To obtain such an order, the government must offer “specific
11 and articulable facts showing that there are reasonable grounds to believe that the
12 contents of a wire or electronic communication, or the records or other
13 information sought, are relevant and material to an ongoing criminal
14 investigation.”²²⁷

15 That standard is lower than the probable cause standard that governs warrants
16 under the Fourth Amendment and Article I, Section 13 of the California
17 Constitution. Nonetheless, the lower standard used for a Section 2703(d) order
18 may be constitutionally permissible if the Fourth Amendment and Article I,
19 Section 13 do not apply.

220. 18 U.S.C. § 2703(b)(1)(B)(i).

221. 18 U.S.C. § 2703(c)(1)(A).

222. 18 U.S.C. § 2703(c)(1)(B).

223. 18 U.S.C. § 2703(c)(2).

224. *Id.*

225. 18 U.S.C. § 2702(b)(8) & (c)(4).

226. 18 U.S.C. § 2702(b)(6) (reporting to National Center for Missing and Exploited Children); (7) (inadvertently obtained evidence of crime).

227. 18 U.S.C. § 2703(d).

1 A Section 2703(d) order can be used to obtain a wide range of stored
2 communications, including stored voice messages, email, text messages, and other
3 writings. The general principle that there is a reasonable expectation of privacy
4 with regard to private conversations would seem to encompass those forms of
5 communications. The only obstacle to there being a reasonable expectation of
6 privacy with respect to those forms of communication is the third party doctrine.

7 As discussed above, it is not clear that the third party doctrine applies to the
8 content of communications. Moreover, there is one decision of the Sixth Circuit
9 Court of Appeals holding that the Stored Communications Act violates the Fourth
10 Amendment to the extent that it permits access to stored email content without a
11 warrant. Finally, recall that Article I, Section 13 of the California Constitution is
12 not subject to a third party exception. Therefore, the use of a Section 2703(d) order
13 would likely violate Article I, Section 13.

14 In light of the foregoing, there is reason to believe that the use of a Section
15 2703(d) order to obtain stored communications is unconstitutional.

16 *Prohibitions on Use of Administrative and Grand Jury Subpoenas*

17 As discussed above, the courts have held that the use of an administrative or
18 grand jury subpoena *duces tecum* to obtain records does not necessarily violate the
19 Fourth Amendment or Article I, Section 13 of the California Constitution.

20 Nonetheless, the Stored Communications Act does not permit the use of such
21 subpoenas to obtain two types of stored information:

- 22 (1) ECS content that has been stored for 180 days or less.
- 23 (2) General non-content information.

24 The prohibition on use of these subpoenas does not affect police searches,
25 because police are not authorized to obtain administrative subpoenas or grand jury
26 subpoenas. The only effect is to prohibit access to such records by administrative
27 agencies and grand juries. It is likely that grand juries can instead access such
28 records by means of a warrant obtained by a district attorney on the grand jury's
29 behalf. But administrative agencies have no way to obtain a general search
30 warrant. This means that administrative agencies are effectively barred from
31 accessing these types of information.

32 The purpose of such a prohibition is not clear. In particular, it is counter-
33 intuitive to allow the use of a subpoena to obtain the content of communications
34 but not allow use of a subpoena to obtain non-content information.

35 *Delayed Notice*

36 Under the Stored Communications Act the use of an administrative or grand jury
37 subpoena is contingent on giving prior notice to the affected customer.²²⁸ Prior
38 notice to the customer is consistent with the notion, discussed above, that the

228. 18 U.S.C. § 2703(b)(1)(B).

1 constitutionality of an investigative subpoena *duces tecum* depends on the fact that
2 the person whose privacy is to be invaded will have notice and an opportunity to
3 be heard before the subpoena operates.

4 However, the Stored Communications Act allows such notice to be delayed, by
5 successive 90 day periods, if a court finds that prior notification would produce
6 any of the following “adverse results:”

- 7 (A) endangering the life or physical safety of an individual;
- 8 (B) flight from prosecution;
- 9 (C) destruction of or tampering with evidence;
- 10 (D) intimidation of potential witnesses; or
- 11 (E) otherwise seriously jeopardizing an investigation or unduly delaying a
12 trial.²²⁹

13 In addition, the government may obtain a court order commanding a service
14 provider not to notify its customer of a warrant, court order, or subpoena issued
15 under the SCA.²³⁰

16 It is not clear whether use of an investigative subpoena *duces tecum*, without
17 prior notice to the customer and an opportunity for the customer to object to the
18 reasonableness of the search, is sufficient to satisfy the requirements of the Fourth
19 Amendment and Article I, Section 13 of the California Constitution.

20 **Preservation of Evidence**

21 The Stored Communications Act provides two ways in which the government
22 can require a communication service provider to secure evidence against
23 destruction by a customer, while the government obtains the necessary
24 authorization for access.

25 First, the government can simply “request” that an ECS or RCS provider
26 “preserve records and other evidence in its possession pending the issuance of a
27 court order or other process.”²³¹ The provider is obliged to do so, for a period of 90
28 days (subject to extension for another 90-day period on the request of the
29 government).²³²

30 Second, if the government is using an administrative subpoena or court order to
31 request access to ECS data that is in electronic storage for more than 180 days, or
32 to request RCS data, it may include in the authorizing instrument a requirement
33 that the service provider create a backup copy of the requested data.²³³ Ordinarily,
34 the customer is given notice of the creation of the backup within three days after

229. 18 U.S.C. § 2705(a)(2).

230. 18 U.S.C. § 2705(b).

231. 18 U.S.C. § 2703(f)(1).

232. 18 U.S.C. § 2703(f)(2).

233. 18 U.S.C. § 2704(a)(1). See also 18 U.S.C. § 2704(a)(1)(a)(3) (retention of backup), (4) (release of backup), (5) (authority to order backup creation to avoid destruction of evidence).

1 the backup copy is created.²³⁴ However, that notice can be delayed if notice would
2 lead to the sort of “adverse results” previously described in the discussion of
3 “Delayed Notice.”²³⁵

4 A customer who receives notice of the creation of a backup may move to quash
5 or vacate the underlying subpoena or order.²³⁶

6 **Cost Reimbursement**

7 In general, the government is required to reimburse a service provider for
8 reasonably necessary costs incurred in “searching for, assembling, reproducing, or
9 otherwise providing” customer information that the provider is compelled to
10 provide.²³⁷

11 **Remedies for Violations**

12 The remedies provided in the Stored Communications Act are the exclusive
13 remedies for a violation of the Act.²³⁸ Notably, the Stored Communications Act
14 does *not* provide for suppression of evidence derived from a violation of the Act
15 (suppression may be available if a violation of the Act is also a violation of the
16 Fourth Amendment).

17 The Act provides for the following types of relief:

- 18 • *Civil Action Generally.* Any person who is aggrieved by a knowing or
19 intentional violation of the Stored Communications Act may bring an action
20 against the violator (other than the United States), seeking preliminary,
21 equitable, or declaratory relief, damages, and attorneys fees and costs.²³⁹
- 22 • *Civil Action Against the United States.* Any person who is aggrieved by a
23 willful violation of the Stored Communications Act by the United States
24 may bring a civil action against the United States for money damages.²⁴⁰
- 25 • *Criminal Penalty.* A person who intentionally accesses a communication
26 facility without sufficient authorization and obtains, alters, or prevents
27 authorized access to a wire or electronic communication may be fined,
28 imprisoned, or both.²⁴¹
- 29 • *Administrative Discipline.* If a court or federal agency finds that an officer
30 or agent of the United States violated the Act, the department may take
31 disciplinary action against the violator.²⁴²

234. 18 U.S.C. § 2704(a)(2).

235. *Id.*

236. 18 U.S.C. § 2704(b).

237. 18 U.S.C. § 2706.

238. 18 U.S.C. § 2708. See also 18 U.S.C. § 2712(d).

239. 18 U.S.C. § 2707(a)-(b).

240. 18 U.S.C. § 2712(a).

241. 18 U.S.C. § 2701(b).

242. 18 U.S.C. § 2707(d).

1 There is no cause of action against a provider, in any court, if the provider acted
2 in accordance with a court order, warrant, subpoena, statutory authorization, or
3 certification pursuant to the Stored Communications Act.²⁴³

4 In addition, good faith reliance on any of the following is a complete defense to
5 any civil or criminal action brought under the Stored Communications Act or any
6 other law:

7 (1) a court warrant or order, a grand jury subpoena, a legislative authorization,
8 or a statutory authorization (including a request of a governmental entity under
9 section 2703(f) of this title);

10 (2) a request of an investigative or law enforcement officer under section
11 2518(7) of this title; or

12 (3) a good faith determination that section 2511(3) of this title permitted the
13 conduct complained of...²⁴⁴

14 Video Privacy Protection Act

15 In 1988, the SCA was amended to add a section that protects the privacy of
16 consumer video rental histories.²⁴⁵ That statute (known as the “Video Privacy
17 Protection Act”) establishes civil liability if a “video tape service provider”
18 discloses customer information that “identifies a person as having requested or
19 obtained specific video materials or services.”²⁴⁶

20 By its terms, this provision applies to “prerecorded video cassette tapes *or*
21 *similar audio visual materials*,” “video tapes *or other audio visual material*,” and
22 to both “goods *and services*.”²⁴⁷ That language seems designed to extend the
23 section’s protections to audio visual content regardless of medium. In fact, there is
24 case law that seems to accept that the statute applies to DVDs.²⁴⁸ Similarly, a
25 district court recently held that the statute applies to video content streamed over
26 the Internet.²⁴⁹

27 There are exceptions to the statute’s prohibition on disclosure where law
28 enforcement obtains a warrant based on probable cause, where a court orders
29 discovery in a civil proceeding, in the ordinary course of business, and where the
30 customer consents to disclosure.²⁵⁰ Moreover, a provider can disclose a customer’s
31 identifying information to any person, so long as the disclosed information does

243. 18 U.S.C. § 2703(e).

244. 18 U.S.C. § 2707(e).

245. 18 U.S.C. § 2710.

246. *Id.*

247. 18 U.S.C. § 2710(a)(1), (3)-(4), (b)(2)(D)(ii).

248. *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th Cir. 2012).

249. *In re Hulu Privacy Litig.*, 2014 U.S. Dist. LEXIS 59479 (N.D. Cal. 2014).

250. 18 U.S.C. § 2710(b).

1 not identify “the title, description, or subject matter of the video” provided to the
2 customer.²⁵¹

3 Disclosure to law enforcement pursuant to a warrant can only be made with
4 prior notice to the customer.²⁵² There is no provision for delayed notice.

5 An aggrieved customer can bring a civil action for damages against a provider
6 who makes an unlawful disclosure.²⁵³

7 Illegally obtained video history information “shall not be received in evidence in
8 any trial, hearing, arbitration, or other proceeding in or before any court, grand
9 jury, department, officer, agency, regulatory body, legislative committee, or other
10 authority of the United States, a State, or a political subdivision of a State.”²⁵⁴

11 Finally, the statute imposes a duty on providers to destroy customer history
12 information “as soon as practicable,” but in no case more than one year from the
13 date it is no longer needed for the purpose for which it was collected.²⁵⁵

14 Pen Register Act

15 Another component of ECPA is the Pen Register Act, which governs the use of
16 “pen registers”²⁵⁶ and “trap and trace devices”²⁵⁷ to collect non-content “dialing,
17 routing, addressing, or signaling information” about wire and electronic
18 communications. A pen register tracks outgoing communications. A trap and trace
19 device tracks incoming communications.

20 **Prohibition and Exceptions**

21 It is generally unlawful for any person to install and use a pen register or trap
22 and trace device.²⁵⁸

23 That general prohibition is subject to a number of exceptions. Some of the
24 exceptions relate to matters that are not germane to state and local agency
25 surveillance, such as exceptions for the collection of information pursuant to the
26 legitimate business needs of a service provider²⁵⁹ and foreign intelligence
27 gathering.²⁶⁰ An exception for use of a pen register or trap and trace device by
28 federal and state law enforcement is discussed further below.

251. 18 U.S.C. § 2710(b)(2)(D).

252. 18 U.S.C. § 2710(b)(3).

253. 18 U.S.C. § 2710(c).

254. 18 U.S.C. § 2710(d).

255. 18 U.S.C. § 2710(e).

256. 18 U.S.C. § 3127(3).

257. 18 U.S.C. § 3127(4).

258. 18 U.S.C. § 3121(a).

259. 18 U.S.C. § 3121(b).

260. 18 U.S.C. § 3121(a).

1 **Government Surveillance Pursuant to Court Order**

2 The federal and state governments can apply to a court of competent jurisdiction
3 for an order authorizing the use of a pen register or a trap and trace device.²⁶¹ A
4 warrant is not required.

5 To apply for an order authorizing the use of a pen register or a trap and trace
6 device, the government must certify that the “information likely to be obtained”
7 pursuant to the order is “relevant to an ongoing criminal investigation being
8 conducted by that agency.”²⁶²

9 If the court finds that the officer submitting the application has made the
10 required certification, the court *shall* issue the order.²⁶³ Consequently, “judicial
11 review is ministerial, and the issuing judge does not conduct an independent
12 inquiry into the facts attested to by the applicant.”²⁶⁴

13 The statute protects the secrecy of the use of a pen register or a trap and trace
14 device, in two ways:²⁶⁵

- 15 • The court order authorizing use is sealed.
- 16 • The court order prohibits any service provider from disclosing the use of the
17 pen register or trap and trace device to any person.

18 A government agency that is authorized to use a pen register or a trap and trace
19 device must use reasonably available technology to prevent the acquisition of
20 communication content.²⁶⁶

21 If a government agency is authorized to use a pen register or a trap and trace
22 device and the agency requests (and the court orders) assistance from a
23 communication service provider, landlord, custodian, or other person, that person
24 is required to provide any information, facilities, and technical assistance
25 necessary to accomplish the installation of the device unobtrusively and with a
26 minimum of service disruption.²⁶⁷

27 Persons who are required to provide assistance are entitled to compensation of
28 their reasonable expenses.²⁶⁸

29 **Emergency Exception**

30 A government agency is not required to obtain an authorizing court order before
31 using a pen register or trap and trace device if (1) there is an emergency situation

261. *Id.*

262. 18 U.S.C. § 3122(b)(2).

263. 18 U.S.C. § 3123(a)(1)-(2).

264. *Electronic Surveillance*, *supra* note 154, at 4:84 (footnotes omitted).

265. 18 U.S.C. § 3123(d).

266. 18 U.S.C. § 3121(c).

267. 18 U.S.C. § 3124(a)-(b).

268. 18 U.S.C. § 3124(c). See also 18 U.S.C. § 3125(d).

1 that requires such use before an order could, with due diligence, be obtained, and
2 (2) there are grounds for issuance of such an order.²⁶⁹ For the purposes of this
3 exception, an emergency situation is one that involves any of the following:

- 4 (A) immediate danger of death or serious bodily injury to any person;
- 5 (B) conspiratorial activities characteristic of organized crime;
- 6 (C) an immediate threat to a national security interest; or
- 7 (D) an ongoing attack on a protected computer (as defined in section 1030) that
8 constitutes a crime punishable by a term of imprisonment greater than one year
9²⁷⁰

10 If an agency proceeds under this exception, it is required to obtain a court order
11 within 48 hours after the installation of the device.²⁷¹ In the absence of such an
12 order, use of the device must end at the earliest of the 48-hour period, the refusal
13 of the court to grant the order, or the acquisition of the information sought.²⁷²

14 The knowing failure to apply for an order authorizing emergency use within the
15 48-hour period specified above is a violation of the statute.²⁷³

16 **Remedy for Violation**

17 A person who knowingly violates the prohibition on installation and use of a pen
18 register or a trap and trace device may be fined, imprisoned for not more than one
19 year, or both.²⁷⁴ There does not appear to be any civil remedy.

20 Moreover, if an investigative or law enforcement officer willfully discloses a
21 record obtained with a pen register or a trap and trace device, other than in the
22 official performance of duties, the disclosure is deemed to be a violation of the
23 Stored Communications Act.²⁷⁵ The remedies for a violation of the Stored
24 Communication Act are discussed earlier in this report.

25 There is no cause of action in any court against a communication provider (or its
26 personnel) for providing assistance in accordance with a court order or request
27 pursuant to the statute.²⁷⁶ Good faith reliance on a court order or request under The
28 Pen Register Act is a complete defense against any civil or criminal action brought
29 under any law.²⁷⁷

269. 18 U.S.C. § 3125(a).

270. 18 U.S.C. § 3125(a)(1).

271. 18 U.S.C. § 3125(a).

272. 18 U.S.C. § 3125(b).

273. 18 U.S.C. § 3125(c).

274. 18 U.S.C. § 3121(d).

275. 18 U.S.C. § 2707(g). This rule does not apply to records that were previously lawfully disclosed by the government or by the plaintiff in a civil suit. *Id.*

276. 18 U.S.C. § 3124(d).

277. 18 U.S.C. § 3124(e).

1 **Pen Register Act and Article I, Section 13 of the California Constitution**

2 Pen registers and trap and trace devices collect telephone number dialing
3 information. This is exactly the kind of metadata that was at issue in *Smith v.*
4 *Maryland*.²⁷⁸ In that case, the court held that there was no reasonable expectation
5 of privacy with respect to such information, because it had been voluntarily
6 disclosed to a third party.

7 Telephone number dialing information was also at issue in *California v. Blair*,²⁷⁹
8 a case in which the California Supreme Court did not apply the federal third party
9 doctrine to Article I, Section 13 of the California Constitution. It held that there
10 can be a reasonable expectation of privacy with regard to telephone dialing
11 information for the purposes of Article I, Section 13. Consequently, it appears that
12 the use of a pen register or trap and trace device without a warrant would violate
13 the California Constitution.²⁸⁰

14 **Location Tracking**

15 Can the ECPA statutes discussed above be used by the government to access
16 customer location data? The answer is complicated and somewhat uncertain.

17 First, a distinction must be drawn between *historical* location data and data that
18 is *real-time or prospective*. Most of the reported cases focus on the latter, but there
19 are cases holding that *historical* data can be accessed under the Stored
20 Communication Act.²⁸¹ The argument seems to be that cell phone location data is
21 “a record or other information pertaining to a subscriber to or customer of” an
22 ECS or RCS provider.²⁸² However, the general purpose of the Stored
23 Communications Act is to obtain existing stored records, not to gather information
24 prospectively.²⁸³

25 In most cases, the government would use a pen register or a trap and trace
26 device to gather prospective non-content data about customer communications.

278. 442 U.S. 735 (1979).

279. 25 Cal. 3d 640 (1979).

280. That was also the opinion of the California Attorney General in two opinions addressing the matter. See 69 Ops. Cal. Atty. Gen. 55 (1986). See also 86 Ops. Cal. Atty. Gen. 198 (2003) (“Search warrants issued by a court and subpoenas issued either by a court or grand jury are normally available to authorize the placement of pen registers and trap and trace devices in California.”).

281. See, e.g., *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

282. 18 U.S.C. § 2703(c).

283. See, e.g., *In re Application for Pen Register and Trap/Trace Device With Cell Site Location and Auth.*, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (“[T]he entire focus of the [Stored Communications Act] is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the [Stored Communications Act] contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.”).

1 The statute governing such devices specifically provides for the collection of
2 “signaling information,”²⁸⁴ which appears to encompass cell site location data.²⁸⁵
3 On its face, that language suggests that a pen register could be used to track real-
4 time and prospective cell site location data.

5 However, the Communications Assistance for Law Enforcement Act includes
6 language that presents an obstacle to such use of a pen register. That statute, which
7 requires telecommunication providers to make their systems technically accessible
8 to government surveillance, provides in part:

9 (a) Capability requirements . . . [A] telecommunications carrier shall ensure that
10 its equipment, facilities, or services that provide a customer or subscriber with the
11 ability to originate, terminate, or direct communications are capable of -

12 . . .

13 (2) expeditiously isolating and enabling the government, pursuant to a court
14 order or other lawful authorization, to access call-identifying information that is
15 reasonably available to the carrier -

16 (A) before, during, or immediately after the transmission of a wire or electronic
17 communication (or at such later time as may be acceptable to the government);
18 and

19 (B) in a manner that allows it to be associated with the communication to which
20 it pertains, *except that, with regard to information acquired solely pursuant to the*
21 *authority for pen registers and trap and trace devices (as defined in section 3127*
22 *of Title 18), such call-identifying information shall not include any information*
23 *that may disclose the physical location of the subscriber (except to the extent that*
24 *the location may be determined from the telephone number).*²⁸⁶

25 In response to that apparent restriction on the use of a pen register to gather
26 location information, the government has emphasized the use of the word “solely”
27 in the phrase “information acquired *solely* pursuant to the authority for pen
28 registers and trap and trace devices.” The government has argued that use of a pen
29 register to acquire such information is permissible if coupled with some other
30 source of authority. Specifically, it has been argued that a pen register can be used
31 to gather location information if the applicant obtains an order to obtain non-
32 content information under the Stored Communications Act. This requires a higher
33 evidentiary showing than under the Pen Register Act, but does not require a
34 warrant based on probable cause. The federal courts have split on whether the
35 government’s “hybrid” or “converged” authority argument is plausible. Most
36 courts have rejected it, holding that there is no authority under ECPA to gather

284. 18 U.S.C. § 3127(3)-(4).

285. See, e.g., *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register*, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) (“cell site location data is encompassed by the term ‘signaling information.’”).

286. 47 U.S.C. § 1002 (emphasis added).

1 prospective location data.²⁸⁷ But a few courts have accepted the argument and have
2 issued orders accordingly.²⁸⁸

3 The statutory arguments discussed above may have been partially superseded by
4 the United States Supreme Court. In the fairly recent case of *United States v.*
5 *Jones*,²⁸⁹ the Court held that the use of a GPS tracking device without a warrant
6 violated the Fourth Amendment of the United States Constitution. Although the
7 Court did not decide how the Fourth Amendment would apply to location tracking
8 using cell site or GPS location data that is obtained from a communication service
9 provider, five concurring Justices indicated, in *dicta*, that such tracking could be a
10 Fourth Amendment search.²⁹⁰ The Fourth Amendment status of such a search
11 would depend on the duration of tracking and the severity of the crime.²⁹¹ The
12 concurring Justices did not offer a bright line standard, but did state that
13 warrantless location tracking conducted on the facts before the Court (four weeks
14 of tracking in a routine drug trafficking case) would have violated the Fourth
15 Amendment.²⁹²

OTHER FEDERAL PRIVACY STATUTES

16
17 There are a number of federal statutes that do not directly regulate government
18 surveillance practices, but that restrict the disclosure of certain information in
19 order to protect personal privacy. If such statutes apply to the states, they can
20 operate as an additional restriction on government access to customer information
21 of communication service providers. The most important statutes of that type are
22 discussed below.

Health Insurance Portability and Accountability Act of 1996

23
24 The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”),²⁹³
25 addresses a number of issues relating to health insurance and healthcare
26 administration. HIPAA requires the Secretary of Health and Human Services to
27 adopt regulations protecting the privacy of individual healthcare information.²⁹⁴

287. See generally Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use, 15 A.L.R. Fed. 2d 537 (2014).

288. *Id.*

289. 132 S. Ct. 945 (2012).

290. See generally CLRC Staff Memorandum 2014-13, pp. 35-39.

291. *Id.*

292. *Id.*

293. P.L. 104-191 (1996).

294. *Id.* at § 264.

1 The key requirements of those regulations (hereafter the “HIPAA Privacy
2 Rule”²⁹⁵) are discussed below.

3 The HIPAA Privacy Rule generally prohibits the disclosure of protected health
4 information by covered entities and their business associates.²⁹⁶ “Protected health
5 information” is a defined term, which is in turn comprised of a series of other
6 nested definitions.²⁹⁷ For present purposes, it is sufficient to say that protected
7 health information generally means information, in any form, created or received
8 by specified entities, that relates to health condition, treatment, or payment for
9 treatment, and that either identifies the subject of the information or makes it
10 reasonably possible to determine that person’s identity.²⁹⁸

11 The general prohibition is subject to a number of exceptions. Many of the
12 exceptions relate to health care administration. Exceptions for government access
13 that appear to be relevant to this study include the following:

- 14 • *Disclosure required by law.*²⁹⁹ Information may be disclosed if the
15 disclosure is required by law (e.g., legally required disclosure of suspected
16 abuse, neglect, domestic violence,³⁰⁰ certain serious wounds,³⁰¹ or
17 communicable disease exposure³⁰²).
- 18 • *Use in adjudicative proceeding.* Information may be disclosed pursuant to a
19 court order (or order of an administrative tribunal) in the course of a judicial
20 or administrative proceeding.³⁰³ Disclosure is also authorized pursuant to a
21 subpoena, discovery request, or other lawful process, without a court order,
22 provided that notice was given to the subject of the requested information or
23 the disclosed information is subject to a protective order that limits its
24 use.³⁰⁴
- 25 • *Court-ordered law enforcement access.*³⁰⁵ Information may be disclosed to
26 law enforcement pursuant to a court order, court-ordered warrant, or
27 subpoena or summons issued by a judicial officer.
- 28 • *Grand jury subpoena.*³⁰⁶

295. 45 C.F.R. § 164.500 *et seq.* See also 45 C.F.R. § 160.101 *et seq.*

296. 45 C.F.R. § 164.502(a).

297. See C.F.R. § 160.103 (defining “protected health information,” “individually identifiable health information,” and “health information”).

298. *Id.*

299. 45 C.F.R. § 164.512(a).

300. 45 C.F.R. § 164.512(c).

301. 45 C.F.R. § 164.512(f)(1)(i).

302. 45 C.F.R. § 164.512(b)(1)(iv).

303. 45 C.F.R. § 164.512(e)(i).

304. 45 C.F.R. § 164.512(e)(ii).

305. 45 C.F.R. § 164.512(f)(1)(ii)(A).

306. 45 C.F.R. § 164.512(f)(1)(ii)(B).

- 1 • *Administrative request.*³⁰⁷ An administrative subpoena (or similar
2 investigative instrument) can be used to authorize disclosure where the
3 information sought is “relevant and material to a legitimate law enforcement
4 inquiry,” the request is specific and limited, and “de-identified” information
5 could not be used.
- 6 • *Incapacitated person suspected of being victim of crime.*³⁰⁸
- 7 • *Decedent suspected of being victim of crime.*³⁰⁹
- 8 • *Evidence of crime on disclosing entity’s premises.*³¹⁰
- 9 • *Information regarding patient identity and location.*³¹¹
- 10 • *Healthcare emergency.*³¹² In a healthcare emergency, information may be
11 disclosed to law enforcement if necessary to alert law enforcement to the
12 commission of a crime, the location of a victim, or the identity, description,
13 or location of the perpetrator.
- 14 • *Serious threat to health and safety.*³¹³ Information may be disclosed based
15 on a good faith belief that disclosure will prevent or lessen a serious and
16 imminent threat to health or safety, or to identify or apprehend a violent
17 criminal or a person who has escaped from a correctional facility.

18 Cable Communication Policy Act of 1984

19 The Cable Communication Policy Act of 1984 (“CCPA”)³¹⁴ is another important
20 federal privacy statute. It generally forbids a cable operator from disclosing
21 personally identifiable information about a subscriber, without the subscriber’s
22 consent.³¹⁵

23 The CCPA’s general prohibition on the disclosure of subscriber information is
24 subject to exceptions, the most relevant being an exception for disclosure to law
25 enforcement pursuant to a court order.³¹⁶

26 A showing of probable cause is not required for the issuance of such an order.
27 Instead, the government need only show “clear and convincing evidence that the
28 subject of the information is reasonably suspected of engaging in criminal activity
29 and that the information sought would be material evidence in the case....”³¹⁷

307. 45 C.F.R. § 164.512(f)(1)(ii)(C)

308. 45 C.F.R. § 164.512(f)(3)(ii).

309. 45 C.F.R. § 164.512(f)(4).

310. 45 C.F.R. § 164.512(f)(5).

311. 45 C.F.R. § 164.512(f)(2).

312. 45 C.F.R. § 164.512(f)(6).

313. 45 C.F.R. § 164.512(j).

314. 47 U.S.C. ch. 5, subch. V–A.

315. 47 U.S.C. § 551(c).

316. 47 U.S.C. § 551(c)(2)(B), (h).

317. 47 U.S.C. § 551(h)(1).

1 However, the subject of the order must be given an opportunity to appear and
2 oppose the issuance of the order.³¹⁸

3 Privacy Protection Act of 1980

4 The Privacy Protection Act of 1980 (“PPA”)³¹⁹ is a federal privacy statute that
5 restricts police searches of the work product and other documentary materials of a
6 journalist.

7 The PPA generally prohibits the following:

8 Notwithstanding any other law, it shall be unlawful for a government officer or
9 employee, in connection with the investigation or prosecution of a criminal
10 offense, to search for or seize any work product materials possessed by a person
11 reasonably believed to have a purpose to disseminate to the public a newspaper,
12 book, broadcast, or other similar form of public communication, in or affecting
13 interstate or foreign commerce...³²⁰

14 A similar prohibition applies to “documentary materials, other than work
15 product materials.”³²¹

16 The PPA’s general prohibitions do not apply if there is “probable cause to
17 believe that the person possessing such materials has committed or is committing
18 the criminal offense to which the materials relate...”³²²

19 That exception is subject to a further narrowing exception. It does not apply if
20 the crime being investigated “consists of the receipt, possession, communication,
21 or withholding of such materials or the information contained therein.”³²³
22 However, that limitation is itself subject to exceptions. It does not apply if the
23 information sought relates to national defense, classified data, specified restricted
24 data, or child pornography.³²⁴

25 There is also an exigency exception if there is reason to believe that immediate
26 seizure is necessary to prevent death or serious bodily injury.³²⁵ If the material to
27 be seized is not work product, the general prohibition is also subject to exceptions
28 where disclosure is sought for the following purposes:

- 29
- To prevent the destruction, alteration, or concealment of the documents.³²⁶

318. 47 U.S.C. § 551(h)(2).

319. 42 U.S.C. § 2000aa.

320. 42 U.S.C. § 2000aa(a).

321. 42 U.S.C. § 2000aa(b).

322. 42 U.S.C. § 2000aa(a)-(b).

323. *Id.*

324. *Id.*

325. 42 U.S.C. § 2000aa(a)(2), (b)(2).

326. 42 U.S.C. § 2000aa(b)(3).

- 1 • The California Invasion of Privacy Act,³³⁷ which includes a number of
2 important protections of communication privacy, including a general
3 prohibition on wiretapping and a warrant requirement for location tracking.
- 4 • The California Wiretap Act,³³⁸ which is analogous to the federal Wiretap
5 Act.
- 6 • Penal Code Section 1524(c), which provides a special procedure for the
7 issuance of a warrant that is used to obtain records that are “in the
8 possession or under the control of” an attorney, doctor, psychotherapist, or
9 clergy member.
- 10 • Penal Code Section 1524(g), which provides that no warrant may be issued
11 for records described in Evidence Code Section 1070. That Evidence Code
12 provision protects specified members of the press from contempt for
13 refusing to disclose sources or “unpublished information obtained or
14 prepared in gathering, receiving or processing of information for
15 communication to the public.”
- 16 • The Reader Privacy Act,³³⁹ which protects against government access to
17 user records of a library or other “book service” (including an online
18 provider).
- 19 • Civil Code Section 1799.3, which restricts the disclosure of video sale or
20 rental records.
- 21 • California Right to Financial Privacy Act,³⁴⁰ which restricts government
22 access to customer financial records.
- 23 • The Confidentiality of Medical Information Act,³⁴¹ which regulates the use
24 and disclosure of patient information by a provider of health care.
- 25 • Public Utilities Code Sections 2891 to 2894.10, which provide
26 miscellaneous protections for the privacy of telephone and telegraph
27 company customers.
- 28 • Education Code Sections 49061 to 49085, which regulate the maintenance,
29 use, and disclosure of student records.
- 30 • The Information Privacy Act of 1977,³⁴² which regulates state agency
31 collection and use of personal information.
- 32 • Vehicle Code Section 9951, which regulates the use of a vehicle “recording
33 device.”

34 These statutes should be taken into account, and adjusted if necessary, when
35 revising the laws governing state and local agency access to customer information
36 from a communication service provider.

337. Penal Code § 630 *et seq.*

338. Penal Code § 629.50 *et seq.*

339. Civ. Code §§ 1798.90-1798.90.05; 2011 Cal. Stat. ch. 424.

340. Gov’t Code §§ 7460-7493.

341. Civ. Code §§ 56-56.37. See also Penal Code §§ 1543-1545

342. Civ. Code § 1798 *et seq.*

SUMMARY OF FINDINGS

1
2 The privacy of one’s communications and the protection of that privacy against
3 invasion by the government is a fundamental civil liberty. That right is at the heart
4 of multiple provisions of the federal and state constitutions.

5 The most direct protection of communication privacy can be found in the Fourth
6 Amendment and Article I, Section 13 of the California Constitution. Those
7 provisions protect reasonable expectations of privacy by requiring that any
8 government surveillance of communications be reasonable and providing that any
9 warrant authorizing surveillance be based on a neutral magistrate’s finding of
10 probable cause, with a particular description of the place to be searched and the
11 things to be seized. When surveillance involves an ongoing interception,
12 additional special protections apply.

13 While the search and seizure jurisprudence is still evolving with respect to
14 modern methods of communication, it appears that the Fourth Amendment and
15 Article I, Section 13, *when taken together*, apply to almost all types of electronic
16 communication information, including both content and metadata. The only
17 exception is that there might not be a reasonable expectation of privacy when
18 government tracks a person’s movements within public places for a relatively brief
19 period of time. However, California statutory law was recently amended to require
20 a warrant for all location tracking. **Consequently, in California, it appears that a
21 warrant is generally required for state and local agency access to any type of
22 electronic communication information.**

23 In some circumstances, electronic surveillance could also violate the express
24 right of privacy that is protected in the California Constitution. However, there is
25 authority suggesting that, in the context of a police investigation, the privacy right
26 is coextensive with the right against unreasonable search and seizure. While
27 protection of the constitutional privacy right is undoubtedly important, the
28 application of constitutional search and seizure protections may be sufficient to
29 protect the privacy right. **This provides an independent rationale for applying
30 the requirements of the Fourth Amendment and Article I, Section 13 of the
31 California Constitution to government surveillance of electronic
32 communications.**

33 The same is likely true with regard to the chilling of free expression that
34 government surveillance of communications could cause in some circumstances.
35 Notwithstanding the obvious importance of protecting the right of free expression
36 from government curtailment, the Supreme Court’s decision in *Zurcher v.*
37 *Stanford Daily* suggests that the protections of the Fourth Amendment may be
38 sufficient to safeguard against such harms. **This too provides an independent
39 rationale for applying the requirements of the Fourth Amendment and
40 Article I, Section 13 of the California Constitution to government surveillance
41 of electronic communications.**

1 Federal statutory law on communication surveillance applies to the states. Those
2 statutes appear to provide a minimum level of privacy protection, preempting any
3 less protective state regulation. The federal surveillance statutes are largely
4 consistent with federal and California constitutional requirements, with three
5 possible exceptions:

- 6 • The use of a Section 2703(d) order to obtain stored communications may
7 violate the Fourth Amendment and is likely to violate Article I, Section 13
8 of the California Constitution.
- 9 • The use of a pen register or trap and trace device without a warrant appears
10 to violate Article I, Section 13 of the California Constitution. The same is
11 probably true with regard to any collection of Internet metadata.
- 12 • The use of an investigative subpoena to obtain communications, without
13 advance notice to the person whose communications are to be seized and an
14 opportunity for judicial review before the subpoena operates, may violate
15 the Fourth Amendment and Article I, Section 13 of the California
16 Constitution.

17 This is a tentative report. **The Commission is circulating it for public review**
18 **and comment.** A comment supporting the content of the report is just as important
19 as a comment criticizing the content or suggesting a change. After reviewing any
20 public comments, the Commission may make changes to improve the report. The
21 Commission will then issue a final report and submit it to the Legislature and the
22 Governor.

23 At an appropriate point after it approves a final report, the Commission will
24 begin the process of preparing draft legislation, as directed by the Legislature. The
25 content of the draft legislation will conform to the requirements of constitutional
26 and statutory law, as described in the final report.