Study G-300 March 30, 2015

Memorandum 2015-10

State and Local Agency Access to Customer Information from Communication Service Providers: Staff Draft Tentative Report

At its February meeting, the Commission[1] decided that the next step in its study of *State and Local Agency Access to Customer Information from Communication Service Providers* would be to prepare and distribute a tentative report of its findings regarding the relevant requirements of constitutional law and federal statutory law. The report would not include any reform recommendations or proposed legislation.[2]

A staff draft of such a report is attached for the Commission's review. If the Commission approves the report, with or without changes, the staff will circulate it for a period of public review and comment.

If the report is approved for distribution at the April meeting, the staff recommends that the public comment period end on June 15, 2015. That would provide approximately two months for public review. The Commission could then consider public comment at its August 7, 2015, meeting.

Should the attached draft be circulated as the Commission's tentative report? If so, should any revisions be made? What should be the deadline for public comment?

Respectfully submitted,

Brian Hebert
Executive Director

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

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

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

#G-300

STATE OF CALIFORNIA

CALIFORNIA LAW REVISION COMMISSION

STAFF DRAFT

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 _____.

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

STATE AND LOCAL AGENCY ACCESS TO ELECTRONIC COMMUNICATIONS

SCOPE OF REPORT

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

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

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

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

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

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

In addition, this report does not address access to information through discovery in a civil, criminal, or administrative proceeding. Such access is supervised by the court, which can hear and address any constitutional or statutory objections to the

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

2. *Id*.

disclosure of information. For that reason, discovery does not present the same issues as surveillance conducted as part of a pre-trial investigation.

CONSTITUTIONAL LAW

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

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

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

Those constitutional rights are discussed below.

Search and Seizure

Fourth Amendment of the United States Constitution

The Fourth Amendment of the United States Constitution provides:

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

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

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

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

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

> The amendment itself shows that the search is to be of material things — the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or *things* to be seized.
>
> …
>
> The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants.
>
> By the invention of the telephone fifty years ago and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.
>
> …
>
> Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment. The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here, those who intercepted the projected voices were not in the house of either party to the conversation.[4]

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

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

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

> only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify — a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life — a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. … But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> Moreover, "in the application of a constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping.…[5]

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

Reasonable Expectation of Privacy

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

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

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

> We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the 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).

> constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.[8]

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

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected," because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable. …
>
> The critical fact in this case is that "[o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume" that his conversation is not being intercepted. … The point is not that the booth is "accessible to the public" at other times…, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable. …[9]

As indicated, a "reasonable expectation of privacy" is two-pronged: It requires (1) a subjective expectation of privacy that (2) society considers to be objectively reasonable.[10]

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

Third Parties and the Fourth Amendment

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

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

United States v. Miller

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

In reaching that conclusion, the Court first rejected the argument, grounded in *Boyd v. United States*,[14] that the Fourth Amendment protects against "compulsory production of a man's private papers."[15]

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

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

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. … This Court 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*.

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

Smith v. Maryland

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

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

> First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. … Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[19]
>
> …
>
> [The analysis in *Miller*] dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. … We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[20]

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

---

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

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

Communication Content v. Metadata

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

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

> [A] pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications. This Court recently noted:
>
> "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed — a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *United States v. New York Tel. Co.*, 434 U. S. 159, 167 (1977).

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

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

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

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

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

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

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

Recent Supreme Court Developments

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

---

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

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

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

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

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

More recently, the Court held that the Fourth Amendment applies to a police search of the contents of a cell phone, incident to a lawful arrest.[28] As part of its analysis, the Court analyzed the privacy expectations that a person has with respect to the contents of a cell phone. In its analysis, the Court does not mention that much of the information contained within a cell phone has been voluntarily shared with third parties. Nor did it draw a clear distinction between content and metadata. Significantly, the Court expressly rejected a government-proposed exception to the warrant requirement for phone dialing information. Such an exception would be easily administered and would seem to fall squarely within the ambit of the existing third party doctrine. Importantly, such an exception would 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).

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

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

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

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

Proposition 8 — "Right to Truth-in-Evidence"

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

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

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

The California Supreme Court has made clear that Proposition 8 did not eliminate the substantive right that is provided in Article I, Section 13.[31] It simply narrowed the remedies that are available to address a violation of that right:

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

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).

> through the exclusion of the evidence so obtained, except to the extent that exclusion remains federally compelled.[32]

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

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

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

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

> It cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable. The prosecution concedes as much, although it asserts that this expectation is not constitutionally cognizable. Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential.
>
> … A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.[34]

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

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

Furthermore, records of a customer's financial transactions are an unavoidable part of modern life, which provide a "virtual current biography" of the customer:

> For all practical purposes, the disclosure by individuals or business firms of 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.

> participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.
>
> Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[36]

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

> The rationale of *Burrows* applies in a comparable manner to information regarding charges made by a credit card holder. As with bank statements, a person who uses a credit card may reveal his habits, his opinions, his tastes, and political views, as well as his movements and financial affairs. No less than a bank statement, the charges made on a credit card may provide "a virtual current biography" of an individual. …
>
> A credit card holder would reasonably expect that the information about him disclosed by those charges will be kept confidential unless disclosure is compelled by legal process. The pervasive use of credit cards for an ever-expanding variety of purposes — business, social, personal, familial — and the intimate nature of the information revealed by the charges amply justify this conclusion.[38]

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.

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

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

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

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

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

Additional Considerations in Special Cases

Interception of Communications

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

39. *Id.* at 653.

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

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

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

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

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

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

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

In summary, an interception warrant must meet the general requirements for issuance of a search warrant under the Fourth Amendment, and must also particularly identify the communications that are being sought, limit the duration of the interception (with a new showing of probable cause to justify an extension), and demonstrate sufficient exigency to justify interception without notice to the target of the interception. As discussed later in this report, these so-called "super-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*.

Location Tracking

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

(1) *Cell tower triangulation*. Cell service providers are able to approximate the location of a cell phone, by applying a triangulation algorithm to data about the phone's communication with nearby cell towers.[45]

(2) *Global positioning system (GPS) data*. Many cell phones and other mobile communication devices are capable of determining the precise location of the device by using the GPS satellite system.[46]

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

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

However, there is another potential limitation on a person's reasonable expectations of privacy with regard to location tracking. The United States Supreme Court has held that a person does not have a reasonable expectation of privacy as to the person's movements within a public space. Such movements are open to observation by any person, including police. "A person traveling in an 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.

his movements from one place to another."[48] That limitation on privacy does not apply to information about a person's location within private areas.[49]

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

> The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.
>
> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*…. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant. … We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.
>
> For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.[50]

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

Investigative Subpoena

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

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

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

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

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

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

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

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

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

---

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.").

> A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion. Because this intrusion is both an immediate and substantial invasion of privacy, a warrant may be issued only by a judicial officer upon a demonstration of probable cause — the safeguard required by the Fourth Amendment.
>
> *A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.*
>
> In short, the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded. And while a challenge to a warrant questions the actual search or seizure under the probable cause standard, a challenge to a subpoena is conducted through the adversarial process, questioning the reasonableness of the subpoena's command.[55]

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

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

---

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).

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

Summary of Search and Seizure Requirements

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

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

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

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

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

58. See discussion of "Federal Statutory Law — Intereception of Communications" *infra*.

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

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

Freedom of Expression

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

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

The First Amendment is applicable to the states.[59]

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

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

Government surveillance of electronic communications does not directly restrain speech or association. However, such surveillance could indirectly affect 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.").

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

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

(1) *Associational privacy*. The Internet enables the formation of private groups for the discussion and advancement of ideas. If the government can determine the identity of the participants in an online discussion forum, it could chill the free association of those who wish to "gather" online for the purpose of private group discussions.

(2) *Anonymous speech*. The Internet makes it very easy for a person to make public statements anonymously. If the government can determine the identity of a person associated with an anonymous user name on an Internet discussion forum, that could chill the free expression of those who are only comfortable speaking anonymously.

(3) *Reader privacy*. The Internet is an extremely important source of information and opinion. If the government can access a person's communication data, it could determine what content a person has been reading or viewing. This invasion of a reader's privacy could chill the right to read unpopular or embarrassing material.

(4) *Private speech*. Electronic communications are an increasingly important conduit for protected speech. If government is known to directly monitor electronic communications, that surveillance could have a chilling effect on expressive activity.

(5) *Press confidentiality*. Increasingly, journalists are using the Internet, both as a place to publish and a tool for research and for confidential communication with sources. Government access to a journalist's private electronic communications could reveal confidential sources and methods, chilling press freedom.

Associational Privacy

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

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

> Effective advocacy of both public and private points of view, particularly 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").

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

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

> The fact that Alabama, so far as is relevant to the validity of the contempt judgment presently under review, has taken no direct action … to restrict the right of petitioner's members to associate freely, does not end inquiry into the effect of the production order. … In the domain of these indispensable liberties, whether of speech, press, or association, the decisions of this Court recognize that abridgment of such rights, even though unintended, may inevitably follow from varied forms of governmental action. Thus in *[American Communications Assn.* v. *Douds*, 339 U.S. 382 (1950)], the Court stressed that the legislation there challenged, which on its face sought to regulate labor unions and to secure stability in interstate commerce, would have the practical effect "of discouraging" the exercise of constitutionally protected political rights, … and it upheld the statute only after concluding that the reasons advanced for its enactment were constitutionally sufficient to justify its possible deterrent effect upon such freedoms. Similar recognition of possible unconstitutional intimidation of the free exercise of the right to advocate underlay this Court's narrow construction of the authority of a congressional committee investigating lobbying and of an Act regulating lobbying, although in neither case was there an effort to suppress speech. … The governmental action challenged may appear to be totally unrelated to protected liberties. Statutes imposing taxes upon rather than prohibiting particular activity have been struck down when perceived to have the consequence of unduly curtailing the liberty of freedom of press assured under the Fourteenth Amendment.
>
> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said in *American Communications Assn.* v. *Douds*…: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to

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

> preservation of freedom of association, particularly where a group espouses dissident beliefs.[63]

Based on that reasoning, the Court held that the state court order compelling production of the NAACP's membership list "must be regarded as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association."[64] Such a restraint must be justified by a compelling state interest.[65]

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

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

Anonymous Speech

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

The Court first discussed prior cases in which it held that a complete prohibition on the public distribution of printed literature violated the constitutional right of freedom of speech.[69] It then considered whether a narrower prohibition, on the 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.

The Court had "no doubt" that requiring the source of a pamphlet to be identified "would tend to restrict freedom to distribute information and therefore freedom of expression."[70]

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies, was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books. … Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. … Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.
>
> We have recently had occasion to hold in two cases that there are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. *Bates* v. *Little Rock*, 361 U.S. 516; *N. A. A. C. P.* v. *Alabama*, 357 U.S. 449, 462. The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance. This broad Los Angeles ordinance is subject to the same infirmity. We hold that it, like the Griffin, Georgia, ordinance [generally prohibiting the public distribution of printed literature], is void on its face.[71]

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

Reader Privacy

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

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

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

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

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

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

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

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

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

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

While government access to that type of information would not directly bar a person from accessing particular Internet content, it could have a chilling effect 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.

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

Private Speech

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

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

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

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

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

> The greatly increased "chilling effect" resulting from the latter *governmental* activity brings constitutional considerations into play.[82]

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

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

Press Confidentiality

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

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

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

86. *Id*. at 563-64.

> Properly administered, the preconditions for a warrant — probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness — should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices.
>
> …
>
> The hazards of such warrants can be avoided by a neutral magistrate carrying out his responsibilities under the Fourth Amendment, for he has ample tools at his disposal to confine warrants to search within reasonable limits.[87]

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

Conclusion

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

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

Privacy

"Penumbral" Privacy Right in the United States Constitution

The United States Constitution does not contain express language guaranteeing a general right of privacy. However, there are several cases in which the Supreme Court has found a constitutional right of privacy, either in the "penumbra" of other enumerated constitutional rights, as a liberty interest protected as a matter of substantive due process, or as a right that preceded the Constitution and is 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*).

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

> The association of people is not mentioned in the Constitution nor in the Bill of Rights. The right to educate a child in a school of the parents' choice — whether public or private or parochial — is also not mentioned. Nor is the right to study any particular subject or any foreign language. Yet the First Amendment has been construed to include certain of those rights.
>
> …
>
> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. … Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[91]

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

> The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.[92]

Said another way:

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

The California Supreme Court has described those two types of privacy interests as "informational privacy" and "autonomy privacy," respectively:

> Legally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy"); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy").[94]

Autonomy Privacy

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

> Although "[t]he Constitution does not explicitly mention any right of privacy," the Court has recognized that one aspect of the "liberty" protected by the Due Process Clause of the Fourteenth Amendment is "a right of personal privacy, or a guarantee of certain areas or zones of privacy." Roe v. Wade, 410 U.S. 113, 152 (1973). This right of personal privacy includes "the interest in independence in making certain kinds of important decisions." Whalen v. Roe, 429 U.S. 589, 599-600 (1977). While the outer limits of this aspect of privacy have not been marked by the Court, it is clear that among the decisions that an individual may make without unjustified government interference are personal decisions "relating to marriage, Loving v. Virginia, 388 U.S. 1, 12 (1967); procreation, Skinner v. Oklahoma ex rel. Williamson, 316 U.S. 535, 541-542 (1942); contraception, Eisenstadt v. Baird, 405 U.S., at 453-454; id., at 460, 463-465 (WHITE, J., concurring in result); family relationships, Prince v. Massachusetts, 321 U.S. 158, 166 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925); Meyer v. Nebraska, [262 U.S. 390, 399 (1923)]." Roe v. Wade, supra, at 152-153.[95]

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

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

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

> Nor can it be said that any individual has been deprived of the right to decide independently, with the advice of his physician, to acquire and to use needed medication. Although the State no doubt could prohibit entirely the use of particular Schedule II drugs, it has not done so. This case is therefore unlike those in which the Court held that a total prohibition of certain conduct was an impermissible deprivation of liberty. Nor does the State require access to these drugs to be conditioned on the consent of any state official or other third party. Within dosage limits which appellees do not challenge, the decision to prescribe, or to use, is left entirely to the physician and the patient.
>
> We hold that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either the reputation or the independence of patients for whom Schedule II drugs are medically indicated is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment.[97]

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

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

Informational Privacy

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

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

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

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

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

98. *Id.*

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

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

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

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

> State and lower federal courts have offered a number of different interpretations 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).

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

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

> In two cases decided more than 30 years ago, this Court referred broadly to a constitutional privacy "interest in avoiding disclosure of personal matters." *Whalen* v. *Roe*, 429 U.S. 589, 599-600, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977); *Nixon* v. *Administrator of General Services*, 433 U.S. 425, 457, 97 S. Ct. 2777, 53 L. Ed. 2d 867 (1977). …
>
> We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged portions of the Government's background check do not violate this right in the present case. The Government's interests as employer and proprietor in managing its internal operations, combined with the protections against public dissemination provided by the Privacy Act of 1974, 5 U.S.C. § 552a, satisfy any "interest in avoiding disclosure" that may "arguably ha[ve] its roots in the Constitution." *Whalen*, *supra*, at 599, 605, 97 S. Ct. 869, 51 L. Ed. 2d 64.[106]

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

> As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance.[107]

To summarize, there is no United States Supreme Court precedent that clearly 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.

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

Informational Privacy and the Fourth Amendment

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

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

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

Summary of Federal Constitutional Privacy Right

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

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

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

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

Express Privacy Right in the California Constitution

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

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

That privacy right was added by initiative in 1972.[109]

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

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

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

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

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

111. *Id.* at 761.

The Court held that the Constitution does not invalidate all information gathering, but instead requires that the government show a "compelling justification for such conduct."[112]

In considering the effect of the new privacy right, the Court looked to the election brochure materials for the proposition that created the right, stating that such materials represent "in essence, the only 'legislative history' of the constitutional amendment available to us."[113] The Court noted that it had "long recognized the propriety of resorting to election brochure arguments as an aid in construing legislative measures and constitutional amendments adopted pursuant to a vote of the people."[114]

The Court discussed the election brochure at some length:

> In November 1972, the voters of California specifically amended article I, section 1 of our state Constitution to include among the various "inalienable" rights of "all people" the right of "privacy." Although the general concept of privacy relates, of course, to an enormously broad and diverse field of personal action and belief, the moving force behind the new constitutional provision was a more [focused] privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy.
>
> The principal objectives of the newly adopted provision are set out in a statement drafted by the proponents of the provision and included in the state's election brochure. The statement begins: "The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create "cradle-to-grave" profiles of every American. [para.] *At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian*." (Italics in original.)
>
> The argument in favor of the amendment then continues: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.
>
> "*Fundamental to our privacy is the ability to control circulation of personal information*. [Italics in original.] This is essential to social relationships and personal freedom. The proliferation of government and business records over 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.

> do not know that these records even exist and we are certainly unable to determine who has access to them.
>
> "Even more dangerous is the loss of control over the accuracy of government and business records of individuals. Obviously if the person is unaware of the record, he or she cannot review the file and correct inevitable mistakes. . . . [para.] The average citizen . . . does not have control over what information is collected about him. Much is secretly collected. . . ."
>
> The argument concludes: "The right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is a compelling public need. . . ."[115]

Some important points can be drawn from that discussion:

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

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

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

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

Consequently, there must be a "careful balancing of the right of civil litigants to 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.

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

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

Private Action

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

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

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

Elements of the Privacy Right

In *Hill v. NCAA*, the California Supreme Court took the opportunity to conduct a fairly thorough review of California's constitutional privacy right and its antecedents in the United States Constitution and the common law. After discussing those foundations, the Court set out the elements of a cause of action 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) The identification of a specific legally protected privacy interest.

(2) A reasonable expectation of privacy on the part of the plaintiff.

(3) A "serious" invasion of the protected privacy interest.

Those elements are discussed further below.

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

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

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

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

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

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

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

---

123. *Id*. at 35-36.

124. *Id*. at 36.

125. *Id*.

> The extent of [a privacy] interest is not independent of the circumstances." (*Plante* v. *Gonzalez*, *supra*, 575 F.2d at p. 1135.) Even when a legally cognizable privacy interest is present, other factors may affect a person's reasonable expectation of privacy. For example, advance notice of an impending action may serve to "'limit [an] intrusion upon personal dignity and security'" that would otherwise be regarded as serious. (*Ingersoll* v. *Palmer*, *supra*, 43 Cal.3d at p. 1346 [upholding the use of sobriety checkpoints].)
>
> In addition, customs, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy. (See, e.g., *Whalen*, *supra*, 429 U.S. at p. 602 [51 L.Ed.2d at p. 75] [reporting of drug prescriptions to government was supported by established law and "not meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of health care"]; *Fraternal Order of Police, Lodge No. 5* v. *City of Philadelphia* (3d Cir. 1987) 812 F.2d 105, 114 [no invasion of privacy in requirement that applicants for promotion to special police unit disclose medical and financial information in part because of applicant awareness that such disclosure "has historically been required by those in similar positions"].)
>
> A "reasonable" expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms. (See, e.g., Rest.2d Torts, supra, § 652D, com. c ["The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens."][126]

The Court also noted that advance voluntary consent can affect a person's reasonable expectation of privacy: "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant."[127]

Serious Invasion of Privacy. Finally, the Court held that a constitutional privacy claim must involve a "serious" violation of a legally protected privacy interest. The Court's discussion of this element is short:

> No community could function if every intrusion into the realm of private action, no matter how slight or trivial, gave rise to a cause of action for invasion of privacy. "Complete privacy does not exist in this world except in a desert, and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part." (Rest.2d Torts, *supra*, § 652D, com. c.) Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy.[128]

This might seem to set a fairly high bar for an actionable claim, with the right of privacy only protecting against "an egregious breach of social norms." However,

126. *Id*. at 36-37.

127. *Id*.

128. *Id*. at 37.

the Court quickly revisited the elements described in *Hill v. NCAA* and made clear that they are not as strict as it might appear.

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

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

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

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

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

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

Standard of Review

In *White v. Davis* the Court held that the government must demonstrate a "compelling" public need in order to justify its invasion of the California

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.

Constitution's privacy right.[135] The Court quoted the part of the ballot brochure asserting that "[t]he right of privacy … should be abridged only when there is a compelling public need."[136]

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

> *White* signifies only that some aspects of the state constitutional right to privacy — those implicating obvious government action impacting freedom of expression and association — are accompanied by a "compelling state interest" standard.[137]

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

> The particular context, i.e., the specific kind of privacy interest involved and the nature and seriousness of the invasion and any countervailing interests, remains the critical factor in the analysis. Where the case involves an obvious invasion of an interest fundamental to personal autonomy, e.g., freedom from involuntary sterilization or the freedom to pursue consensual familial relationships, a "compelling interest" must be present to overcome the vital privacy interest. If, in contrast, the privacy interest is less central, or in bona fide dispute, general balancing tests are employed.
>
> For the reasons stated above, we decline to hold that every assertion of a privacy interest under article I, section 1 must be overcome by a "compelling interest." Neither the language nor history of the Privacy Initiative unambiguously supports such a standard. In view of the far-reaching and multifaceted character of the right to privacy, such a standard imports an impermissible inflexibility into the process of constitutional adjudication.[138]

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

> Invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest. Legitimate interests derive from the legally authorized and socially beneficial activities of government and private entities. Their relative importance is determined by their proximity to the central functions of a particular public or private enterprise. Conduct alleged to be an invasion of privacy is to be evaluated based on the extent to which it furthers legitimate and important competing interests.
>
> Confronted with a defense based on countervailing interests, the plaintiff may undertake the burden of demonstrating the availability and use of protective

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).

measures, safeguards, and alternatives to defendant's conduct that would minimize the intrusion on privacy interests.[139]

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

> Judicial assessment of the relative strength and importance of privacy norms and countervailing interests may differ in cases of private, as opposed to government, action.
>
> *First*, the pervasive presence of coercive government power in basic areas of human life typically poses greater dangers to the freedoms of the citizenry than actions by private persons. "The government not only has the ability to affect more than a limited sector of the populace through its actions, it has both economic power, in the form of taxes, grants, and control over social welfare programs, and physical power, through law enforcement agencies, which are capable of coercion far beyond that of the most powerful private actors." (Sundby, *Is Abandoning State Action Asking Too Much of the Constitution?* (1989) 17 Hastings Const. L. Q. 139, 142-143 [hereafter Sundby].)
>
> *Second*, "an individual generally has greater choice and alternatives in dealing with private actors than when dealing with the government." (Sundby, *supra*, 17 Hastings Const.L.Q. at p. 143.) Initially, individuals usually have a range of choice among landlords, employers, vendors and others with whom they deal. To be sure, varying degrees of competition in the marketplace may broaden or narrow the range. But even in cases of limited or no competition, individuals and groups may turn to the Legislature to seek a statutory remedy against a specific business practice regarded as undesirable. State and federal governments routinely engage in extensive regulation of all aspects of business. Neither our Legislature nor Congress has been unresponsive to concerns based on activities of nongovernment entities that are perceived to affect the right of privacy. (See, e.g., Lab. Code, § 432.2, subd. (a) ["No employer shall demand or require any applicant for employment or prospective employment or any employee to submit to or take a polygraph, lie detector or similar test or examination as a condition of employment or continued employment"]; 29 U.S.C. § 2001 [regulating private employer use of polygraph examination].)
>
> *Third*, private conduct, particularly the activities of voluntary associations of persons, carries its own mantle of constitutional protection in the form of freedom of association. Private citizens have a right, not secured to government, to communicate and associate with one another on mutually negotiated terms and conditions. The ballot argument recognizes that state constitutional privacy protects in part "our freedom of communion and our freedom to associate with the people we choose." (Ballot Argument, *supra*, at p. 27.) Freedom of association is also protected by the First Amendment and extends to all legitimate organizations, whether popular or unpopular. (*Britt* v. *Superior Court* (1978) 20 Cal. 3d 844, 854 [143 Cal. Rptr. 695, 574 P.2d 766]; see also Tribe, American Constitutional Law (2d ed. 1988) § 18-2, p. 1691 [noting rationale of federal constitutional requirement of state action protects "the freedom to make certain choices, such as

139. *Id* at 38.

> choices of the persons with whom [one associates]" which is "basic under any conception of liberty"].)[140]

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

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

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

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

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

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

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

140. *Id*. at 38-39.

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

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

> parties to the [conversation] have a 'reasonable expectation of privacy' with respect to what is said…." (*People* v. *Estrada* (1979) 93 Cal.App.3d 76, 98 [155 Cal.Rptr. 731].)[143]

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

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

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

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

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

Summary of California Constitutional Privacy Right

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

In order to "weed out" trivial, insignificant, and de minimis privacy violations, courts first determine whether a privacy right claim meets the following threshold elements: (1) an identifiable privacy interest, (2) a reasonable expectation of privacy, and (3) a serious violation of the privacy interest.

---

143. *Id*. at 629.

144. *Id*. at n.5.

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

146. *Id*. at 1149.

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

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

FEDERAL SURVEILLANCE STATUTES

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

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

ECPA is relevant to the conduct of electronic surveillance in California for two reasons: It expressly applies to the states and it has been held to preempt less protective state laws.[148] Federal preemption is a consequence of the "Supremacy 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 surveillance. As we discussed … the report refers to numerous areas touching upon the field of electronic surveillance which state law may control. Thus, in referring to a need for uniform nationwide standards, it appears that Congress was not expressing an intent to preempt the entire field; rather, it was emphasizing

Interception of Communication Content

As amended by ECPA, the Wiretap Act governs the interception[150] of wire,[151] oral,[152] and electronic communications.[153] The statute generally prohibits the interception of communications and the use of intercepted communications, subject to a number of statutory exceptions. The major elements of the statute are described below.

Meaning of "Interception"

Although the definition of "intercept" is not expressly limited to the acquisition of communication contents during transmission, that was the practical meaning of the term when it was first used in the original wiretap law. At that time, telephone calls and oral conversations were necessarily intercepted while they were occurring, because such communications were not routinely recorded and stored for later access.

Modern electronic communications are different. They are routinely stored and the stored copies can be accessed long after the process of transmission has been completed. Access to such "stored" communications is not considered to be an interception for the purposes of the Wiretap Act. Instead, it is regulated under the Stored Communications Act, which is discussed later in this report.

---

the need to ensure nationwide compliance with the newly declared standards in *Berger* and *Katz*. Accordingly, we conclude that Congress did not intend to occupy the entire field of electronic surveillance to the exclusion of state regulation."). See also CLRC Staff Memorandum 2014-33, pp. 38-51.

149. U.S. Const. art VI, cl. 2 ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.").

150. 18 U.S.C. § 2510(4) ("'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.")

151. 18 U.S.C. § 2510(1) ("'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce").

152. 18 U.S.C. § 2510(2) ("'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication").

153. 18 U.S.C. § 2510(12) ("'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include — (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds").

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

> The term "electronic communication" includes transient electronic storage intrinsic to the transmission of such communications. Thus, an e-mail message continued to be an electronic communication during momentary intervals, intrinsic to the communication process, when the message is in transient electronic storage. Interception of electronic communication occurs with reading of transmissions as they are sent….[154]

Prohibitions and Exceptions

It is generally unlawful to intentionally intercept a wire, oral, or electronic communication.[155] It is also generally unlawful to disclose or use the contents[156] of communications that are known to have been obtained through an unlawful interception or that are disclosed in order to obstruct a criminal investigation.[157] In addition, electronic communication service providers are generally prohibited from divulging the contents of communications, while they are in transmission, to anyone other than the sender or intended recipient.[158] Finally, it is unlawful to manufacture, sell, advertise, or deliver devices designed for surreptitious interception of wire, oral, or electronic communications.[159]

Those general prohibitions are subject to a number of exceptions. Many of the exceptions relate to matters that are not germane to state and local agency surveillance, such as exceptions for the interception of publicly accessible information,[160] interception with the consent of a participant,[161] and interception pursuant to the legitimate business needs of the service provider.[162] There are also exceptions for interception for specified federal purposes.[163] Federal interception is beyond the scope of this report.

---

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. *Id*. at (3)(a).

159. 18 U.S.C. § 2512(1).

160. *Id*. at (2)(g).

161. *Id*. at (2)(c)-(d), (3)(b)(ii).

162. *Id*. at (2)(a)(i)-(ii); (3)(b)(iii).

163. *Id*. at (2)(b) (Federal Communications Commission); (2)(e)-(f) (foreign intelligence gathering).

Government Interception Pursuant to Warrant

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

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

- Interception can only be authorized to investigate specified serious felonies.[166]
- The court must find that other investigative procedures were tried and failed, were unlikely to succeed if tried, or would be too dangerous to try.[167]
- Authorization to intercept communications may not continue "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."[168] However, based on a new showing of probable cause, the court can extend the authorization for one or more additional periods of the same duration.[169]
- The interception must be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under the Wiretap Act.[170]
- The warrant must describe the person whose communications will be intercepted (if known), the communication facilities to be used, the type of communication to be intercepted and the criminal offense to which it relates.[171]
- In addition to finding probable cause for belief that an individual is committing, has committed, or is about to commit a predicate crime, the court must also find "probable cause for belief that particular communications concerning that offense will be obtained through such interception" and "probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be

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. *Id.* at (5).

169. *Id.*

170. *Id.*

171. *Id.* at (4).

intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[172]

- The contents of intercepted communications are required to be recorded in a form that will prevent alteration. On expiration of the period of authorization, the recordings must be made available to the judge.[173]
- Within a reasonable time (not to exceed 90 days) after an authorizing order and any extension of the order has terminated, an "inventory" shall be served on the persons named in the order and on any other party to an intercepted communication as the judge orders, in the interests of justice. The inventory document must provide notice of the interception, including the date and period of interception, and whether any communications were actually intercepted. The judge may also order, in the interests of justice, that portions of the intercepted communications be provided. However, on an ex parte showing of good cause, a judge may postpone service of the inventory.[174]

Exception to Warrant Requirement for Exigent Circumstances

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

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

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

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

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

---

172. *Id.* at (3).
173. *Id.* at (8)(a).
174. *Id.* at (8)(d).
175. *Id.* at (7).
176. *Id.*
177. *Id.*
178. *Id.*

Use of Lawfully Intercepted Communications

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

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

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

Limitations on Use of Intercepted Communications

The contents of a lawfully intercepted communication cannot be introduced into evidence in a proceeding unless all parties receive a copy of the application, as well as the order authorizing the interception, at least 10 days before the proceeding.[185] The judge may waive the 10-day period if it was not possible to provide notice to a party in that time period and the party was not prejudiced.[186]

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

---

179. 18 U.S.C. § 2517(1).
180. *Id*. at (2).
181. *Id*. at (5).
182. *Id*. at (3).
183. *Id*. at (5).
184. *Id*. at (6)-(8).
185. 18 U.S.C. § 2518(9).
186. *Id*.
187. 18 U.S.C. § 2517(4).

Remedies for Violations

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

The act provides for the following types of relief:

- *Injunction*. The United States Attorney General may bring an action to enjoin a felony violation of the Wiretap Act.[189]
- *Suppression of Evidence*. Before any "trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof," an "aggrieved person"[190] may move to suppress the contents of an interception or evidence derived from those contents.[191]
- *Civil Action Generally*. In general, a person whose communication is intercepted, disclosed, or intentionally used in violation of the Wiretap Act, by a person other than the United States, may bring a civil action seeking preliminary or declaratory relief, damages, fees, and costs.
- *Civil Action Against United States*. Any person who is aggrieved by a willful violation of the Wiretap Act by the United States may bring a civil against the United States for money damages.[192]
- *Administrative Discipline*. An officer of the United States who willfully or intentionally violates the chapter may be subject to administrative discipline.[193]
- *Criminal Penalty*. A person who violates the general prohibitions in the Wiretap Act may be punished by a fine, imprisoned for not more than five years, or both.[194]
- *Contempt*. A violation of certain procedures governing law enforcement interception pursuant to court authorization is punishable as contempt.[195]
- *Confiscation of Devices*. Devices that are used, sent, carried, manufactured, assembled, possessed, sold or advertised in violation of the relevant provisions of the Wiretap Act can be seized and forfeited to the United States.[196]

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).

195. 18 U.S.C. § 2518(8)(c).

196. 18 U.S.C. § 2513.

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

Access to Stored Communications

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

Prohibitions and Exceptions

It is generally unlawful to do any of the following:

- Intentionally access an electronic communication service[198] facility, without authorization or in excess of authorization, to obtain, alter, or prevent authorized access to a wire or electronic communication that is in electronic storage.[199]
- For an electronic communication service provider to knowingly divulge, to any person or entity, the contents of a communication that is in electronic storage.[200]
- For a remote computing service[201] provider to knowingly divulge, to any person or entity, the contents of any communication that is "carried or maintained" on the remote computing service on behalf of a customer or subscriber.[202]
- For an electronic communication service provider or a remote computing service provider to knowingly divulge, to any person or entity, a record or other information pertaining to a customer or subscriber.[203]

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 ….").

202. 18 U.S.C. § 2702(a)(2).

203. *Id*. at (a)(3).

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

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

Government Interception Pursuant to Lawful Process

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

- Whether the information sought is held in connection with an "electronic communication service" (hereafter "ECS") or a "remote computing service" (hereafter "RCS").
- If the information is held in connection with an RCS service, whether that service is provided to the general public.
- Whether the information is content or metadata.
- Whether the information has been stored for 180 days or more.

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

ECS v. RCS

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

One potential difficulty with the ECS-RCS dichotomy is that the delivery and receipt of electronic communications also involves the creation and storage of copies. To partially resolve that difficulty, the Stored Communications Act

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.

provides that ECS can include a copy of a message that is in "electronic storage."[208] That term is defined narrowly:

> (17) "electronic storage" means—
> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication ….

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

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

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

RCS Service to the "Public"

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

It does not include an entity that provides service solely on the basis of a special relationship between the entity and the users of the service. For example, a company that provides email service to its employees as an incident of employment would not be providing service to the "public" and so would not be an RCS with regard to its employees.[211]

Some commentators have expressed concern that the definition of "RCS" may exclude universities that provide Internet services to their students, because those

---

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).

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).

services are not being provided to the public generally.[212] If so, the privacy protections afforded to RCS data could be denied to those who receive Internet service from a university or similar entity.

Content and Metadata

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

The SCA also draws a distinction between non-content information generally[214] and a specific subset of non-content information (identifying the customer and detailing the customer's telephone use).[215]

Required Legal Process

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

The forms of legal process that government must use to access different types of 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 • Grand jury or trial subpoena, or • Court order per § 2703(d)[220]

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. *Id*. at (c)(1).

215. *Id*. at (c)(2)

216. 18 U.S.C. § 2703(a).

217. *Id*. at (a) & (b)(1)(A).

218. *Id*. at (b)(1)(B)(i).

219. *Id*. at (a) & (b)(1)(A).

220. *Id*. at (b)(1)(B)(i).

Non-Content Information Generally	• Search warrant,[221] or • Court order per § 2703(d)[222]
Specified Subset of Non-Content Information ("Subscriber Information")	• 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	• No protection under the SCA

In addition, the Stored Communications Act provides an exception for the disclosure of stored communications to address an emergency[225] and miscellaneous other exceptions relating to specific law enforcement situations.[226]

Noteworthy Implications of Existing Statutory Rules

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

Possible Unconstitutionality of Section 2703(d) Order

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

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

A Section 2703(d) order can be used to obtain a wide range of stored communications, including stored voice messages, email, text messages, and other writings. The general principle that there is a reasonable expectation of privacy with regard to private conversations would seem to encompass those forms of

221. *Id.* at (c)(1)(A).

222. *Id.* at (c)(1)(B).

223. *Id.* at (c)(2).

224. *Id.*

225. 18 U.S.C. § 2702(b)(8) & (c)(4).

226. *Id.* at (b)(6) (reporting to National Center for Missing and Exploited Children); (7) (inadvertently obtained evidence of crime).

227. 18 U.S.C. § 2703(d).

communications. The only obstacle to there being a reasonable expectation of privacy with respect to those forms of communication is the third party doctrine.

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

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

Prohibitions on Use of Administrative and Grand Jury Subpoenas

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

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

(1) ECS content that has been stored for 180 days or less.

(2) General non-content information.

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

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

Delayed Notice

Under the Stored Communications Act the use of an administrative or grand jury subpoena is contingent on giving prior notice to the affected customer.[228] Prior notice to the customer is consistent with the notion, discussed above, that the constitutionality of an investigative subpoena *duces tecum* depends on the fact that the person whose privacy is to be invaded will have notice and an opportunity to be heard before the subpoena operates.

228. 18 U.S.C. § 2703(b)(1)(B).

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

> (A) endangering the life or physical safety of an individual;
> (B) flight from prosecution;
> (C) destruction of or tampering with evidence;
> (D) intimidation of potential witnesses; or
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[229]

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

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

Preservation of Evidence

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

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

Second, if the government is using an administrative subpoena or court order to request access to ECS data that is in electronic storage for more than 180 days, or to request RCS data, it may include in the authorizing instrument a requirement that the service provider create a backup copy of the requested data.[233] Ordinarily, the customer is given notice of the creation of the backup within three days after the backup copy is created.[234] However, that notice can be delayed if notice would

229. 18 U.S.C. § 2705(a)(2).

230. *Id*. at (b).

231. 18 U.S.C. § 2703(f)(1).

232. *Id*. at (f)(2).

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

234. *Id*. at (a)(2).

lead to the sort of "adverse results" previously described in the discussion of "Delayed Notice."[235]

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

Cost Reimbursement

In general, the government is required to reimburse a service provider for reasonably necessary costs incurred in "searching for, assembling, reproducing, or otherwise providing" customer information that the provider is compelled to provide.[237]

Remedies for Violations

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

The Act provides for the following types of relief:

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

---

235. *Id*.
236. *Id*. at (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).

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

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

> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);
> (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
> (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of…[244]

Video Privacy Protection Act

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

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

There are exceptions to the statute's prohibition on disclosure where law enforcement obtains a warrant based on probable cause, where a court orders discovery in a civil proceeding, in the ordinary course of business, and where the customer consents to disclosure.[250] Moreover, a provider can disclose a customer's 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. *Id*. at (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).

not identify "the title, description, or subject matter of the video" provided to the customer.[251]

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

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

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

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

Pen Register Act

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

Prohibition and Exceptions

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

That general prohibition is subject to a number of exceptions. Some of the exceptions relate to matters that are not germane to state and local agency surveillance, such as exceptions for the collection of information pursuant to the legitimate business needs of a service provider[259] and foreign intelligence gathering.[260] An exception for use of a pen register or trap and trace device by federal and state law enforcement is discussed further below.

---

251. *Id.* at (b)(2)(D).
252. *Id.* at (b)(3).
253. *Id.* at (c).
254. *Id.* at (d).
255. *Id.* at (e).
256. 18 U.S.C. § 3127(3).
257. *Id.* at (4).
258. 18 U.S.C. § 3121(a).
259. *Id.* at (b).
260. *Id.* at (a).

Government Surveillance Pursuant to Court Order

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

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

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

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

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

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

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

Persons who are required to provide assistance are entitled to compensation of their reasonable expenses.[268]

Emergency Exception

A government agency is not required to obtain an authorizing court order before 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. *Id*. at (c). See also 18 U.S.C. § 3125(d).

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

> (A) immediate danger of death or serious bodily injury to any person;
> (B) conspiratorial activities characteristic of organized crime;
> (C) an immediate threat to a national security interest; or
> (D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year ….[270]

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

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

Remedy for Violation

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

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

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

---

269. 18 U.S.C. § 3125(a).

270. *Id*. at (a)(1).

271. *Id*. at (a).

272. *Id*. at (b).

273. *Id*. at (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. *Id*. at (e).

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

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

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

Location Tracking

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

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

In most cases, the government would use a pen register or a trap and trace 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.").

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

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

> (a) Capability requirements . . . [A] telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of -
>
> . . .
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier -
>
> (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
>
> (B) in a manner that allows it to be associated with the communication to which it pertains, *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)*.[286]

In response to that apparent restriction on the use of a pen register to gather location information, the government has emphasized the use of the word "solely" in the phrase "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices." The government has argued that use of a pen register to acquire such information is permissible if coupled with some other source of authority. Specifically, it has been argued that a pen register can be used to gather location information if the applicant obtains an order to obtain non-content information under the Stored Communications Act. This requires a higher evidentiary showing than under the Pen Register Act, but does not require a warrant based on probable cause. The federal courts have split on whether the government's "hybrid" or "converged" authority argument is plausible. Most 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).

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

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

OTHER FEDERAL PRIVACY STATUTES

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

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[293] addresses a number of issues relating to health insurance and healthcare administration. HIPAA requires the Secretary of Health and Human Services to 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.

The key requirements of those regulations (hereafter the "HIPPAA Privacy Rule"[295]) are discussed below.

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

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

- *Disclosure required by law*.[299] Information may be disclosed if the disclosure is required by law (e.g., legally required disclosure of suspected abuse, neglect, domestic violence,[300] certain serious wounds,[301] or communicable disease exposure[302]).
- *Use in adjudicative proceeding*. Information may be disclosed pursuant to a court order (or order of an administrative tribunal) in the course of a judicial or administrative proceeding.[303] Disclosure is also authorized pursuant to a subpoena, discovery request, or other lawful process, without a court order, provided that notice was given to the subject of the requested information or the disclosed information is subject to a protective order that limits its use.[304]
- *Court-ordered law enforcement access*.[305] Information may be disclosed to law enforcement pursuant to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer.
- *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. *Id*. at (c).

301. *Id*. at (f)(1)(i).

302. *Id*. at (b)(1)(iv).

303. *Id*. at (e)(i).

304. *Id*. at (e)(ii).

305. *Id*. at (f)(1)(ii)(A).

306. *Id*. at (f)(1)(ii)(B).

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

Cable Communication Policy Act of 1984

The Cable Communication Policy Act of 1984 ("CCPA")[314] is another important federal privacy statute. It generally forbids a cable operator from disclosing personally identifiable information about a subscriber, without the subscriber's consent.[315]

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

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

---

307. *Id*. at (f)(1)(ii)(C)
308. *Id*. at (f)(3)(ii).
309. *Id*. at (f)(4).
310. *Id*. at (f)(5).
311. *Id*. at (f)(2).
312. *Id*. at (f)(6).
313. *Id*. at (j).
314. 47 U.S.C. ch. 5, subch. V–A.
315. 47 U.S.C. § 551(c).
316. *Id*. at (c)(2)(B), (h).
317. *Id*. at (h)(1).

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

Privacy Protection Act of 1980

The Privacy Protection Act of 1980 ("PPA")[319] is a federal privacy statute that restricts police searches of the work product and other documentary materials of a journalist.

The PPA generally prohibits the following:

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

A similar prohibition applies to "documentary materials, other than work product materials."[321]

The PPA's general prohibitions do not apply if there is "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate…."[322]

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

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

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

---

318. *Id*. at (h)(2).
319. 42 U.S.C. § 2000aa.
320. *Id*. at (a).
321. *Id*. at (b).
322. *Id*. at (a)-(b).
323. *Id*.
324. *Id*.
325. *Id*. at (a)(2), (b)(2).
326. *Id*. at (b)(3).

- To seize materials that have not been produced in response to a lawful subpoena, after the exhaustion of all appellate remedies.[327]

Family Education Rights and Privacy Act of 1974

The Family Education Rights and Privacy Act of 1974 ("FERPA")[328] is another federal privacy statute that states must comply with in drafting legislation on government access to electronic communications. Among other things, FERPA protects the privacy of student education records.[329]

Schools that are subject to FERPA must have written permission from a student's parent in order to release any information from a student's educational record.[330]

That general restriction is subject to a number of exceptions, including several that involve a disclosure to government. Those exceptions address:

- Disclosure to the juvenile justice system, to serve the student's needs.[331]
- Disclosure to respond to an emergency.[332]
- Disclosure pursuant to a grand jury subpoena.[333]
- Disclosure pursuant to a subpoena issued for law enforcement purposes.[334]
- Disclosure to a child welfare agency.[335]
- Disclosure pursuant to a court order or lawfully issued subpoena, with advance notice to the student's parents (except in cases of suspected child abuse).[336]

BRIEF LIST OF CALIFORNIA PRIVACY STATUTES

As noted earlier, this report does not closely examine California statutes that protect information privacy. Such statutes are subject to change by the Legislature and Governor and so do not constrain the preparation of reform legislation in California.

However, in the interest of completeness, it is worth briefly noting some of the more significant California privacy statutes:

---

327. *Id.* at (b)(4).
328. 20 U.S.C. § 1232g.
329. *Id.*
330. *Id.*
331. *Id.* at (b)(1)(E)(ii).
332. *Id.* at (b)(1)(I).
333. *Id.* at (b)(1)(J)(i).
334. *Id.* at (b)(1)(J)(ii).
335. *Id.* at (b)(1)(L).
336. *Id.* at (b)(2).

- The California Invasion of Privacy Act,[337] which includes a number of important protections of communication privacy, including a general prohibition on wiretapping and a warrant requirement for location tracking.
- The California Wiretap Act,[338] which is analogous to the federal Wiretap Act.
- Penal Code Section 1524(c), which provides a special procedure for the issuance of a warrant that is used to obtain records that are "in the possession or under the control of" an attorney, doctor, psychotherapist, or clergy member.
- Penal Code Section 1524(g), which provides that no warrant may be issued for records described in Evidence Code Section 1070. That Evidence Code provision protects specified members of the press from contempt for refusing to disclose sources or "unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public."
- The Reader Privacy Act,[339] which protects against government access to user records of a library or other "book service" (including an online provider).
- Civil Code Section 1799.3, which restricts the disclosure of video sale or rental records.
- California Right to Financial Privacy Act,[340] which restricts government access to customer financial records.
- The Confidentiality of Medical Information Act,[341] which regulates the use and disclosure of patient information by a provider of health care.
- Public Utilities Code Sections 2891 to 2894.10, which provide miscellaneous protections for the privacy of telephone and telegraph company customers.
- Education Code Sections 49061 to 49085, which regulate the maintenance, use, and disclosure of student records.
- The Information Privacy Act of 1977,[342] which regulates state agency collection and use of personal information.
- Vehicle Code Section 9951, which regulates the use of a vehicle "recording device."

These statutes should be taken into account, and adjusted if necessary, when revising the laws governing state and local agency access to customer information 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

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

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

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

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

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

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

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

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

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