Study G-300 March 28, 2014

Memorandum 2014-13

State and Local Agency Access to Customer Information from Communication Service Providers: Constitutional Issues

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

(1) Modernize the law.
(2) Protect customers' constitutional rights.
(3) Enable state and local agencies to protect public safety.
(4) Clarify procedures.

Memorandum 2014-5 introduced the study and proposed an overall organizational plan for conducting it. The Commission approved the proposed plan.[2] This memorandum begins the first step in that plan, analysis of the constitutional rights that are at issue in this study.

After briefly discussing the application of the California Constitution, this memorandum examines constitutional protections against unreasonable search and seizure. Other constitutional rights, relating to free expression, free association, and privacy, will be discussed in future memoranda.

This memorandum does not examine statutory rules on government access to customer information of communication service providers. Nor does it discuss policy arguments on how the law should regulate this topic. Those discussions

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

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

2. See Minutes (Feb. 2014), p. 4.

will also follow later in the study. At this point, the staff is focused solely on describing the applicable constitutional search and seizure doctrines.

The content of the memorandum is organized as follows:

The staff would like to thank King Hall Law School student Emily Jeng for her contributions to this memorandum. Ms. Jeng is currently serving as a Commission extern.

The Commission invites public input on the matters discussed in this memorandum and any other point that is relevant to this study. Any interested person or group can submit formal comment to the Commission, either in

writing or at a meeting. The staff is also open to receiving informal input, and is willing to meet with any interested group.[3]

APPLICATION OF CALIFORNIA CONSTITUTION

Before analyzing the specific constitutional protections that are relevant to this study, it is worth briefly discussing the application of the California Constitution.

As a general principle, "[r]ights guaranteed by [the California] Constitution are not dependent on those guaranteed by the United States Constitution."[4] This means that the California Constitution can afford greater protections than the United States Constitution. Consequently, the California Constitution must be analyzed separately, to determine whether its requirements are different from those of the United States Constitution.

In 1990, the voters approved Proposition 115. Among other things, that initiative added the following language to Section 24 of Article 1 of the California Constitution:

> In criminal cases the rights of a defendant to equal protection of the laws, to due process of law, to the assistance of counsel, to be personally present with counsel, to a speedy and public trial, to compel the attendance of witnesses, to confront the witnesses against him or her, to be free from unreasonable searches and seizures, to privacy, to not be compelled to be a witness against himself or herself, to not be placed twice in jeopardy for the same offense, and to not suffer the imposition of cruel or unusual punishment, shall be construed by the courts of this State in a manner consistent with the Constitution of the United States. This Constitution shall not be construed by the courts to afford greater rights to criminal defendants than those afforded by the Constitution of the United States, nor shall it be construed to afford greater rights to minors in juvenile proceedings on criminal causes than those afforded by the Constitution of the United States.[5]

That language purports to limit certain constitutional rights of criminal defendants (and minors in juvenile proceedings) to the rights afforded by the United States Constitution. Under that provision, the California Constitution

3. On March 5, 2014, the staff met informally with attorneys from the American Civil Liberties Union and the Electronic Frontier Foundation, at the request of those groups. While there is no obligation to disclose such meetings, the staff will do so in the interest of transparency.

4. Cal. Const. art. 1, § 24.

5. Prop. 115 (June 5, 1990).

could not afford greater rights. If that were the case, there would be no need to analyze California Constitutional rights as part of this study. They would be wholly subsumed within the relevant federal constitutional protections.

However, shortly after the approval of Proposition 115, the California Supreme Court struck down the language set out above.[6] The Court concluded that the new language made a "revision" to the Constitution, which could not be effected through the initiative process.[7]

Given that decision, it appears that the California Constitution can still afford greater protections to criminal defendants than those provided by the United States Constitution. Consequently, state constitutional rights remain relevant to this study and will need to be analyzed separately.

That said, there is one further wrinkle that needs to be noted. In 1982, the voters approved Proposition 8, which added Section 28 of Article 1 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.[8]

As a consequence of that new right, relevant evidence that is obtained in violation of the California Constitution is admissible, unless it falls within an exception to Section 28 or it was also obtained in violation of the United States Constitution.[9] This did not change the substantive scope of the *protections* afforded by the California Constitution; it simply narrowed the *remedies* available to address a violation of a Constitutional 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

6. Raven v. Deukmejian, 52 Cal. 3d 336 (1990).
7. *Id.* at 342.
8. Cal. Const. art 1, § 28(f)(2).
9. In re Lance W., 37 Cal. 3d 873 (1985).

> created *remedy* for violations of the federal or state constitutions, through the exclusion of the evidence so obtained, except to the extent that exclusion remains federally compelled.[10]

The limitation on the remedies available for a violation of the California Constitution does not eliminate the relevance of the California Constitution to this study. Any statute that the Commission recommends must be in accord with the substantive requirements of the California Constitution.

SEARCH AND SEIZURE GENERALLY

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.

The Fourth Amendment is enforceable against the states.[11]

Section 13 of Article 1 of the California Constitution provides a very similar protection:

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

In general, this memorandum only discusses the California Constitution where its requirements are different from those of the United States Constitution.

Most of the discussion that follows concerns the *scope* of the constitutional search and seizure provisions — what constitutes a "search" for the purposes of those provisions? The memorandum then briefly summarizes the *substantive effect* of the search and seizure provisions — when a search occurs, what do the constitutional provisions require?

This memorandum only examines those aspects of search and seizure jurisprudence that appear to be relevant to this study. Elements of search and seizure law that do not bear on the matters at issue in this study are not discussed (e.g., there is no discussion of vehicle searches).

---

10. *Id.* at 886-87.
11. See Mapp v. Ohio, 367 U.S. 643, 655 (1961).

The Fourth Amendment Protects Persons, Places, and Things

When the Fourth Amendment to the United States Constitution was ratified, electronic communications did not exist. All searches and seizures were material and necessarily involved some kind of physical 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*,[12] 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:

> 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.
>
> …

12. 277 U.S. 438 (1928).

> 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.[13]

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 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

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

> 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.…[14]

The narrow trespass-based approach taken to wiretapping in *Olmstead* prevailed until 1967, when the Supreme Court decided *Katz v. United States*.[15]

The Fourth Amendment Protects Reasonable Expectations 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*,[16] 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 constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to

14. *Id.* at 473-75 (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349 (1910)) (citations omitted).
15. 389 U.S. 347 (1967).
16. 316 U.S. 129 (1942).

> achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.[17]

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. …[18]

As indicated, a "reasonable expectation of privacy" is two-pronged; it requires a subjective expectation of privacy that society considers to be objectively reasonable.[19]

Trespass Doctrine Not Displaced by *Katz*

In *United States v. Jones*,[20] the court considered whether the placement of a GPS tracking device on the undercarriage of a car constituted a "search" within the meaning of the Fourth Amendment. The Court found that there was a search, because the placement of the device on a private car constituted a trespass

17. *Katz*, 389 U.S. at 353.
18. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
19. See also Burrows v. Super. Ct., 13 Cal. 3d 238 (1974) (applying reasonable expectation of privacy test to Section 13 of Article 1 of the California Constitution).
20. 132 S. Ct. 945 (2012).

against a person's "effects." In discussing that holding, the Court explained that *Katz* had supplemented the earlier trespass-based understanding of the Fourth Amendment, without replacing it: the "reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[21] In other words, "*Katz* did not narrow the Fourth Amendment's scope."[22]

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.

THIRD PARTY DOCTRINE

In *Katz*, the court held that there was a reasonable expectation of privacy as to words spoken within a closed telephone booth: "One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[23]

The logic of that holding does not seem to depend on the use of any particular communication technology. What mattered was that Katz was in a place where it was reasonable to expect his conversation to be private. It therefore seems logical to extend the same general principle to any type of communication, so long as there is good reason to expect that the communication will be private. Under that reasoning, a cell phone call conducted within a closed telephone booth would seem to be constitutionally indistinguishable from the calls made on the payphone in *Katz*.

However, there may be special characteristics of particular modes of communication that are incompatible with a reasonable expectation of privacy. For example, early cell phones relied on unencrypted radio transmissions that could be intercepted by any person with an off-the-shelf radio scanner. A person using such a cell phone probably wouldn't have a reasonable expectation of privacy, even if making the call within a closed telephone booth.[24]

---

21. *Id.* at 952 (emphasis in original).
22. *Id.* at 951. See also *id.* at 955 (Sotomayor, J., concurring) ("As the majority's opinion makes clear, however, *Katz's* reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.")
23. *Katz*, 389 U.S. at 352.
24. See, e.g., Price v. Turner, 260 F.3d 1144, 1148 (9th Cir. 2001) (no reasonable expectation of privacy in conversation over cordless telephone that was "readily susceptible to interception").

This section of the memorandum discusses one important limitation on reasonable expectations of privacy that appears to be common to all of the methods of communication at issue in this study: the third party doctrine.

Third Parties and the Fourth Amendment

The Supreme Court has held, under what has come to be known as the "third party doctrine," that there is no reasonable expectation of privacy with regard to information that is voluntarily provided to a third party. Consequently, government access to such information is not a search for the purposes of the Fourth Amendment. The third party doctrine developed out of two cases decided in the 1970s, *United States v. Miller*[25] and *Smith v. Maryland*.[26]

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 the defendant'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…."[27]

In reaching that conclusion, the Court first rejected the argument, grounded in *Boyd v. United States*,[28] that the Fourth Amendment protects against "compulsory production of a man's private papers."[29]

> Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks.[30]

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."[31] 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."[32]

25. 425 U.S. 435 (1976).
26. 442 U.S. 735 (1979).
27. *Miller*, 425 U.S. at 440.
28. 116 U.S. 622 (1886).
29. *Id.* at 440.
30. *Id.*
31. *Id.* at 442.
32. *Id.*

> 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 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 likely had no subjective expectation of privacy as to the numbers he dialed and, moreover, any such expectation would not be one that society is prepared to recognize as reasonable.

> 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.[33]

Citing the reasoning in *United States v. Miller*, discussed above, the Court explained why there is no reasonable expectation of privacy regarding numbers dialed on a telephone:

> [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,

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

> 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.[34]

Communicative Content

In *Smith*, the Court emphasized that a pen register does not involve the interception of the *content* of a telephone call:

> [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).
>
> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.[35]

This suggests that there may be a material distinction, for the purposes of the third party doctrine, between content and non-content information. Merely retrieving the numbers dialed on a telephone is like viewing the address written on the outside of an envelope; it tells nothing about the content of the letter inside. By contrast, intercepting the content of a telephone call is clearly a Fourth Amendment search, as would also be the case if the government opened an undelivered letter and read the contents inside the envelope.[36]

---

34. *Id.* at 744-45 (citations omitted).
35. *Smith*, 442 U.S. at 741-42 (emphasis in original).
36. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy. … Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.").

One difficulty with that theory is that it cannot be easily squared with the holding in *Miller*. In that case, the Court held that there is no reasonable expectation of privacy in one's bank records. Such records do indeed contain content.

In any event, the Court has not yet expressly held that there is a distinction, for the purposes of the third party doctrine, between the interception of content and non-content information.

Third Parties and the California Constitution

Importantly, the California Supreme Court has *not* followed the third party doctrine in construing the California Constitution. In fact, the California Supreme Court has reached very different results on issues that are quite similar to those presented in *Miller* and *Smith*.

In *Burrows v. Superior Court*,[37] which preceded *Miller*, the California Supreme Court held that one does have a reasonable expectation of privacy with regard to 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.[38]

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

37. 13 Cal. 3d 238 (1974).
38. *Id.* at 243.

> 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.[39]

Furthermore, records of 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 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.[40]

In *California v. Blair*,[41] 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:

---

39. *Id.* at 244.
40. *Id.* at 247-48.
41. 25 Cal. 3d 640 (1979).

> 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.[42]

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

> [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."[43]

In *People v. Chapman*,[44] 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 may 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.

42. *Id.* at 652.
43. *Id.* at 653.
44. 36 Cal. 3d 98 (1984).

- 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 "current virtual biography." Such information is deserving of protection from unreasonable government intrusion.

Those principles must be borne in mind when evaluating whether government access to customer records of a communications service provider would be a search under the California Constitution.

Third Parties and Modern Technology

Justice Sotomayor has, in *dicta*, expressed doubts about the continued merit of the federal third party doctrine in the age of modern communication technologies:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., *Smith*, 442 U. S., at 742; *United States v. Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," … and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U. S., at 351–352 ("[W]hat [a person]

> seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").[45]

While that discussion signals some potential for change to the federal third party doctrine in the future, for now it is settled law.

JUDICIAL RESTRAINT IN ADDRESSING TECHNOLOGICAL CHANGE

The United States Supreme Court appears to be reluctant to fashion broad precedents on the application of the Fourth Amendment to new and emerging communication technologies.

In *City of Ontario v. Quon*,[46] the Court reversed a Ninth Circuit decision finding that there was a reasonable expectation of privacy in text messages sent and received using an employer-provided device. The Supreme Court did not reach the merits of that issue, instead deciding the case on narrower grounds.

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. … In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. … It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. … Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. … At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.
>
> [The] Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as

45. *Jones*, 132 S. Ct. 945 (2012) (Sotomayor, J. concurring).
46. 500 U.S. 746 (2010).

> reasonable. … Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.
>
> A broad holding concerning employees' privacy expectations *vis-a-vis* employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.…[47]

In *United States v. Jones*,[48] Justice Alito expressed similar caution, suggesting that the Legislature is in the best position to address shifting expectations of privacy in a time of rapid technological change:

> [T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.
>
> On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law. In an ironic sense, although *Katz* overruled *Olmstead*, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress, see 277 U. S., at 465–466, has been borne out.
>
> …

47. *Id.* at 759-60.
48. Discussed in "Third Party Doctrine and Modern Technology" *supra*.

> Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.
>
> Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users — and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.
>
> …
>
> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case — constant monitoring of the location of a vehicle for four weeks — would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. … A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.[49]

"SEARCHES" AND MODERN COMMUNICATION METHODS

This section of the memorandum considers, for different types of modern communication, whether government access to customer information would be a

49. *Jones*, 132 S. Ct. 945 (2012) (Alito, J., concurring).

constitutionally cognizable search. For the most part, there are no directly controlling Supreme Court precedents on these issues. Instead, it is necessary to make reasoned predictions about the application of decisions addressing relevant principles.

Audio and Visual Communication

Katz made clear that the Fourth Amendment protects the privacy of intangible oral communications. In *Berger v. New York*, the Court held that the Fourth Amendment applies to a wiretap of a landline telephone.[50]

Does the same hold true for audio and visual communications conducted using new technologies? For example:

- *Mobile phones*: Mobile telephones are now in widespread use. They provide the same type of real-time audio conversation as a landline telephone, but the signals are transmitted through a terrestrial cell site network or (less commonly) through an orbiting satellite.
- *VOIP*: Voice over Internet Protocol (VOIP) is directly analogous to traditional landline telephone service. The difference — which may be unknown and undetectable to a user — is that the signals are transmitted digitally across the Internet rather than being transmitted over the public telephone network.
- *Video conferencing*. Similar to voice over IP, there are now several services that provide real-time voice and video communication over the Internet.

The staff did not find any decision of the Supreme Court or a federal appellate court that directly addresses these more modern forms of communication. That may be because the wiretapping provisions of the federal Electronic Communications Protection Act generally treat the interception of "electronic communications" in the same way that it does traditional "wire" communications (and the use of listening devices to intercept "oral communications"):

> Congress has by statute aligned the interception of electronic communications with the use of wiretaps to obtain wire communications and the use of electronic listening devices to obtain oral communications. To engage in such conduct, officials generally must seek a court order. Because such an order is sufficient to overcome an expectation of privacy, courts have not

50. 388 U.S. 41 (1967).

> addressed the application of the Fourth Amendment to electronic communications in transmission.[51]

This makes it unnecessary to litigate the matter under the Fourth Amendment.

Why might Congress have afforded the same treatment of telephone wiretaps, eavesdropping on oral communication, and the interception of electronic communications? All seem to share one constitutionally relevant trait, they all involve expectations of "conversational privacy."

> Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. … Our decision in *Katz* refused to lock the Fourth Amendment into instances of actual physical trespass. Rather, the Amendment governs "not only the seizure of tangible items, but extends as well to the recording of oral statements . . . without any 'technical trespass under … local property law.'" That decision implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.[52]

Recall that *Katz* involved the placement of a "bug" on the outside of a telephone booth, to record one end of the telephone conversations held within. It did not involve a wiretap. This suggests that one's reasonable expectation of conversational privacy does not, in general, depend on the use of any particular communication medium.

That said, are there characteristics of particular types of audio or visual communication that might defeat a reasonable expectation of privacy?

Quite probably, yes. As discussed earlier in the memorandum, early model cell phones used unencrypted radio signals that could be intercepted using inexpensive off-the-shelf devices. There would seem to be no reasonable expectation of privacy when using such a communication method. Contemporary cell phones use encrypted digital transmission methods that mostly eliminate the risk of unauthorized interception of signals. However, new technologies have since emerged that allow users to mimic cell towers and trick cell phones into providing user content. Such devices are reportedly being used

51. Carr & Bellia, *The Law of Electronic Surveillance* § 1:9 (2013).
52. United States v. U.S. Dist. Court, 407 U.S. 297, 312-313 (1972).

by several California police departments.[53] If this type of interception becomes commonplace, the expectation of privacy in cell phone calls may be diminished.

Text-Based Messaging

Electronic mail (hereafter "email") is different from real-time streaming audio and video conversations because it involves a serial exchange of written texts, which are delivered through a chain of intermediaries, with copies stored at various points along the way.

The staff did not find any Supreme Court opinion directly deciding whether the Fourth Amendment applies to email or other text based messaging systems.

There appears to be only one federal appellate court decision directly on point: *United States v. Warshak*.[54] In that Sixth Circuit case, the court held that there is a reasonable expectation of privacy with regard to email.

Before discussing the details of *Warshak*, it is worth noting that the Eleventh Circuit had briefly reached a different conclusion, holding that there is no reasonable expectation of privacy in email once it has been delivered.[55] However, that holding was vacated on rehearing just a few months later. In the substitute opinion, the court endorsed the Supreme Court's "disinclination" to establish broad precedents on the application of the Fourth Amendment to emerging communication technologies.[56] The court found narrower grounds on which to decide the case, making no decision on whether the Fourth Amendment applies to email.[57]

United States v. Warshak

In *Warshak*, the defendant argued that the government's warrantless seizure of some 27,000 email messages directly from an Internet service provider violated the Fourth Amendment's prohibition on unreasonable searches and seizures. The court found that Warshak had "plainly manifested" a subjective expectation of privacy with regard to his email. The more difficult question was

53. See <http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spying-technology-used-throughout-northern-california/6144949/>
54. 631 F.3d 266 (6th Cir. 2010).
55. Rehberg v. Paulk, 598 F.3d 1268 (11th Cir. 2010).
56. Rehberg v. Paulk, 611 F.3d 828, 844-46 (11th Cir. 2010).
57. *Id.* at 846. For the purposes of the qualified immunity issue that the court was deciding, it was sufficient to find only that the application of the Fourth Amendment to email has not been "clearly established."

whether that expectation was one that society is prepared to recognize as reasonable.[58]

> This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. *Cf. Katz*, 389 U.S. at 352 (suggesting that the Constitution must be read to account for "the vital role that the public telephone has come to play in private communication"). Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.
>
> In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. *See ibid.; United States v. U. S. Dist. Court*, 407 U.S. 297, 313, 92 S. Ct. 2125, 32 L. Ed. 2d 752 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."). Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States*, 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1007 (2010) (arguing that "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment").[59]

58. *Warshak*, 631 F.3d at 284.
59. *Id.* at 284-85.

The court analogized email to two more traditional forms of communication, telephone calls and mailed letters.

With regard to telephone calls, the court noted that *Katz* established "the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means."[60] This is true, the court notes, notwithstanding the fact that a telephone company can monitor and record calls.[61]

The court then noted that mailed letters receive similar protection. "This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private."[62]

Based on those analogies, the court concluded that email also deserved protection against government access:

> Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 135 (2008) (recognizing the need to "eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other"); *City of Ontario v. Quon*, 130 S. Ct. 2619, 2631, 177 L. Ed. 2d 216 (2010) (implying that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line"); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that "[t]he privacy interests in [mail and email] are identical"). Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification." *Quon*, 130 S. Ct. at 2630. It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve. *See U.S. Dist. Court*, 407 U.S. at 313; United States v. Waller, 581 F.2d 585, 587 (6th Cir. 1978) (noting the Fourth Amendment*'s* role in protecting "private communications"). As some forms of

60. *Id.* at 285.
61. *Id.*
62. *Id.*

> communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise. *See Warshak I*, 490 F.3d at 473 ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.").
>
> If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call — unless they get a warrant, that is. *See Jacobsen*, 466 U.S. at 114; *Katz*, 389 U.S. at 353. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.[63]

The court rejected an argument that defendant had no reasonable expectation of privacy because the ISP's subscriber agreement had reserved the right to access customer emails for certain purposes. The court noted that telephone companies also have the right to monitor calls in some situations, and this is not sufficient to extinguish the reasonable expectation of privacy in telephone calls. However, the court conceded the possibility that the terms of a particular subscriber agreement might be sufficiently intrusive to "snuff out" users' reasonable expectation of privacy.[64]

Ultimately, the court held:

> a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP." … The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. … Moreover, to the extent that the [Stored Communications Act] purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.[65]

63. *Id.* at 285-86.
64. *Id.* at 287.
65. *Id.* at 288.

Third Party Doctrine

One potential weakness of the decision in *Warshak* is that it is not squarely in accord with the existing third party doctrine. Recall that "[w]hat a person knowingly exposes to the public … is not a subject of Fourth Amendment protection."[66] *Miller* applied that principle to conclude that one has no reasonable expectation of privacy in bank records. *Smith* extended the doctrine to numbers dialed on a telephone. Arguably, the same principle could be asserted to argue that there is no reasonable expectation of privacy in email that one voluntarily submits to an ISP.

The fact that email are provided to an ISP for a limited purpose (delivery) would not seem to defeat the third party argument. In both *Miller* and *Smith*, it was expected that the information was being provided for a limited purpose and would not be shared beyond what was necessary to achieve that purpose. The Supreme Court expressly considered that point and still held that disclosure defeated the reasonable expectation of privacy. The same point could be made with regard to email. Employees at an ISP have the ability and perhaps the right under some agreements to read the content of email that they store and deliver. The sender takes the risk that the ISP's personnel will do so and, in some circumstances, might turn over the information to the government.

In anticipation of the third party doctrine argument, the *Warshak* court attempted to distinguish email from the bank records in *Miller*:

> First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. … Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." … By contrast, Warshak received his emails through NuVox. NuVox was an *intermediary*, not the intended recipient of the emails. *See* Bellia & Freiwald, *Stored E-Mail*, 2008 U. Chi. Legal F. at 165 ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests."). Thus, *Miller* is not controlling.[67]

The staff agrees that email is distinguishable from bank records for the reason noted above — the bank in *Miller* was the intended recipient of the information,

66. *Miller*, 425 U.S. at 442.
67. *Warshak*, 631 F.3d at 288 (emphasis in original).

not merely an *intermediary* acting to facilitate communication with another person. By contrast, an ISP is an intermediary.

However, it is not clear whether that distinction can be used to reconcile *Warshak* with *Smith*. In *Smith*, the third party doctrine was applied to the collection of telephone dialing information provided to the telephone company. The telephone company was clearly an intermediary, just like an ISP that is delivering email. If there is no reasonable expectation of privacy in information provided to the telephone company as intermediary, why is the result different when an ISP acts as intermediary?

Perhaps the answer is that the telephone dialing information provided in *Smith* did not include the *content* of the communication. Clearly, under *Katz*, the interception of the *content* a telephone call is a Fourth Amendment search (notwithstanding the fact that such content is voluntarily provided to the telephone company acting as a third party intermediary). As discussed earlier, it may be that the third party doctrine simply does not apply to communicative content. Given that the Supreme Court has not yet addressed that issue expressly, caution counsels against assuming the existence of such an exception.

Recall, however, that the third party doctrine has been held inapplicable to the search and seizure provisions of the California Constitution. The reasoning underlying those cases seems equally applicable to email:

- Email is submitted to an ISP for an expressly limited purpose: delivery. There is no expectation that an ISP will provide the content of one's email to outsiders (absent legal compulsion to do so). Moreover, it is likely that most subscriber agreements guarantee the privacy of user content.[68]
- Email is becoming as ubiquitous and unavoidable as banking or the use of the telephone. If submitting information to one's bank or telephone company is not entirely "volitional," then the same is probably true of submitting email to one's ISP.
- The content of email can reveal a broad array of intimate details of one's private life, creating a "current virtual biography."

For those reasons, it seems likely that the involvement of an ISP as intermediary would not be a bar to a reasonable expectation of privacy under the California Constitution.

68. On the other hand, it was recently revealed that Microsoft had searched a subscriber's email inbox for evidence of a leak of proprietary information. The search may have been authorized under Microsoft's privacy policy. See <http://www.businessinsider.com/microsoft-email-search-legal-statement-2014-3>.

Other Text-Based Communications

Email is not the only method by which private written messages can be sent and received electronically. Other methods include:

- *Text messaging*. "Texting" originally referred to messages sent from one mobile phone device to another, over a telephone network. Once limited to short written messages, text messages can now also be used to send pictures and video files.
- *Internet-based messaging systems.* There are a wide range of Internet-based applications that can send and receive written messages. For example, Facebook has its own messaging system that is very similar to email. And many websites provide person-to-person "chat" tools.

In the staff's view, these text-based messaging methods are functionally equivalent to email for the purposes of Fourth Amendment analysis. In both cases, text is being delivered, through intermediaries who may make copies at various stages of the process. Users are likely to expect that the content of their messages are private (and user agreements likely guarantee that privacy). And such communication is increasingly ubiquitous and highly personal:

> [T]ext message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.[69]

Although its decision was later reversed (in order to avoid deciding the constitutional question), the Ninth Circuit had reached a similar conclusion about the privacy of text messages:

> We see no meaningful difference between [email] and the text messages at issue here. Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, … we also see no meaningful distinction between text messages and letters. As with letters and e-mails, it is not reasonable to expect privacy in the information used to "address" a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider.[70]

69. *Quon*, 500 U.S. at 759-60.
70. Quon v. City of Ontario, 529 F.3d 892, 905 (9th. Cir. 2008) (footnotes omitted) (reversed).

Metadata

The word "metadata" means "data about data."[71] In the context of electronic communications, "metadata" is commonly used to refer to information about a communication, as distinguished from the content of the communication.

A classic example of metadata is the information gathered by a pen register (i.e., the numbers dialed on a telephone). Telephone metadata might also include the date, time, and duration of calls.

With regard to Internet-based communications, metadata could include sender and recipient email addresses; the address of any website visited; the name, type, and size of any file accessed or transmitted; and the identity associated with a particular email address or user name.

In *Smith v. Maryland*,[72] the Court found no subjective or reasonable expectation of privacy in telephone metadata because that information is voluntarily provided to a third party.

Although there is no Supreme Court decision directly on point, federal circuit courts have applied the third party doctrine to Internet metadata. For example, in *United States v. Forrester*,[73] police requested that an ISP install a "mirror port" to track information about the defendant's Internet usage. The mirror port "enabled the government to learn the to/from addresses of [defendant's] e-mail messages, the IP addresses of the websites that [defendant] visited and the total volume of information sent to or from his account."[74] After reiterating the holding of *Smith*, that the use of a pen register is not a Fourth Amendment search, the Ninth Circuit held that the government's use of the mirror port was "constitutionally indistinguishable from the use of a pen register":

> First, e-mail and Internet users, like the telephone users in *Smith,* rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. … Analogously, e-mail and Internet users have no expectation of privacy in the to/from

71. See <http://www.techterms.com/definition/metadata> ("Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.").
72. 442 U.S. 735 (1979).
73. 512 F. 3d 500 (9th Cir. 2008).
74. *Id*. at 505.

> addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers. …
>
> Second, e-mail 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.
>
> The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties.[75]

Despite applying the third party doctrine to email metadata and the IP addresses of visited websites, the court expressed some trepidation about extending the same principle to the addresses of particular web pages:

75. *Id*. at 510-11 (footnotes omitted).

> Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed.[76]

Because the treatment of metadata in *Forrester* was grounded in the federal third party doctrine, the results are likely to be different under the California Constitution. As discussed above, the increasing ubiquity of Internet communication, the expectation that ISPs will use information only for limited purposes and will not share that information with outsiders, and the potential that Internet metadata would reveal a "current virtual biography" of a user would likely lead to the same treatment of Internet metadata that has been afforded telephone metadata. In both cases, the fact that a third party acts as intermediary for the limited purpose of facilitating communication would not affect one's reasonable expectation of privacy under the California Constitution.

Location Tracking

There are currently two general ways that 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 its communication with nearby cell towers.[77]

76. *Id*. at 510, n.6.

77. 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.").

(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.[78]

The United States Supreme Court has not yet decided whether the protections of the Fourth Amendment apply generally to location data accessed from communication service providers. As discussed earlier, the Court came close to addressing that issue in *United States v. Jones*, but decided the case on other grounds (the attachment of a GPS tracking device to the exterior of a car was a trespass against effects and therefore within the traditional scope of the Fourth Amendment).

As discussed below, however, there are strong indications as to how the Court might view the collection of location data directly from a communication service provider (i.e., through cell tracking or the collection of GPS data from a mobile communication device). Those indicators include cases on the use of radio tracking devices ("beepers") and the concurring opinions in Jones.

"Beeper" Cases

A key issue relating to the privacy of location data is the fact that one's movements in public places are not actually private. When a person is walking or driving on a public way, anyone else nearby can directly observe the person's movements. "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[79]

Assuming that there is no physical trespass involved, does this mean that the police may use an electronic tracking device to follow a person's movements without obtaining a warrant?

That question was addressed in a pair of cases involving the placement of a radio tracking device in containers of chemicals used in the manufacture of illegal drugs: *United States v. Knotts*[80] and *United States v. Karo*.[81] Importantly, the beepers were placed in the containers, with the consent of the owner, *before* they were transferred to the person who was tracked. In *Karo*, the Court held that this

78. *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.").

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

80. *Id.*

81. 468 U.S. 705 (1984).

did not involve a trespass.[82] This left the question of whether *use* of a beeper to determine a person's location violates that person's reasonable expectation of privacy.

In *Knotts*, the beeper was not relied on exclusively to determine the suspect's location. Instead, police followed the defendant by more traditional methods ("tailing" in cars, with the assistance of a helicopter). The beeper was used as an aid to that process. The Court observed that a person does not generally have a reasonable expectation of privacy when traveling in a car on a public roadway:

> When [defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[83]

The type of surveillance conducted with the beeper could have been achieved without the beeper. The beeper did not reveal any information that could not have been discovered through direct observation:

> Visual surveillance from public places along [defendant's] route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [defendant's] automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[84]

Karo presented similar facts, with one significant difference. The beeper was not used merely as an aid in traditional methods of "tailing" a suspect. Instead, it was used to independently determine the location of the container of chemicals in which it had been placed. In other words, the police did not follow the container as it was moved from place to place. Instead, they occasionally used the beeper to determine the container's location. Significantly, the beeper at times revealed that the container was located within a private residence.

Based on that distinction, the Court held that the use of the beeper violated the Fourth Amendment:

---

82. *Id.* at 712-13.
83. *Knotts*, 460 U.S. at 282.
84. *Id.*

> This case … presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does.
>
> At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances.[85]

Taken together, *Knotts* and *Karo* suggest that there is generally no reasonable expectation of privacy as to one's location when in a public place, but there is a reasonable expectation of privacy when in a private place.

Concurring Opinions in Jones

As discussed earlier, the majority opinion in *Jones* did not discuss whether location tracking using cell triangulation or GPS data from a mobile device is a search under the Fourth Amendment. It instead decided the case on narrower, trespass-based grounds.

In a concurring opinion authored by Justice Alito and joined by three other justices,[86] the trespass basis for the majority opinion was criticized as antiquated and artificial. Instead, the concurring justices would have analyzed "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[87] This is significant, because the same considerations would seem to apply to any type of location tracking, including government access of a customer's location data from a communication service provider.

Justice Alito's analysis focuses on the practicability of conducting long-term tracking by traditional means:

> 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.

85. *Karo*, 468 U.S. at 714-15.
86. Justices Breyer, Ginsburg, and Kagan.
87. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

> 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.[88]

The point seems to be that there is no reasonable expectation of privacy in one's movements *if it would have been practicable for police to monitor those movements using traditional methods*. Thus, the Fourth Amendment does not govern short-term location monitoring or longer-term monitoring in sufficiently important cases (where the police would have been motivated to use extraordinary resources). In those instances, police could have used traditional methods to follow a suspect, defeating any reasonable expectation of privacy in the target's location.

Presumably, this practicability standard only applies to movements in public places, where traditional police surveillance methods could have been used. Pursuant to *Karo*, use of technology to track movements on private property would probably be a search under the Fourth Amendment. This prospect seems much more likely to arise when tracking a cell phone or other mobile device, than when tracking a vehicle.

88. *Id.* at 964.

Under the facts presented in *Jones* — continuous location monitoring for over four weeks in a drug trafficking case — the concurring justices would have found a violation of the Fourth Amendment, even if the location data had been obtained through non-trespassory means.

In a separate concurrence, Justice Sotomayor joined the majority in holding that the existence of a trespass was sufficient to establish a Fourth Amendment violation. "The reaffirmation of that principle suffices to decide this case."[89]

However, she also agreed with the other concurring justices that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"[90]

> [As] Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance. … With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. … In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." … As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. … Under that rubric, I agree with Justice Alito that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[91]

She goes on to explain why even short-term location monitoring might violate reasonable expectations of privacy:

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, *e.g.*, *People v. Weaver*, 12 N. Y. 3d 433, 441-442, 909 N.E.2d 1195, 1199, 882 N.Y.S.2d 357 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS

89. *Id.* at 955 (Sotomayor, J., concurring).
90. *Id.*
91. *Id.*

> treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. … And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois v. Lidster*, 540 U.S. 419, 426, 124 S. Ct. 885, 157 L. Ed. 2d 843 (2004).
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring — by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track — may "alter the relationship between citizen and government in a way that is inimical to democratic society."
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. … I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance…".[92]

If the concurring opinions authored by Justices Alito and Sotomayor are read together, it would appear that there are currently five votes on the Court for the proposition that non-trespassory cell-phone or GPS tracking is a violation of reasonable expectations of privacy *in some circumstances*. It is not clear where the lines would be drawn, but it seems certain that four weeks of monitoring in a routine drug trafficking case would be considered a search under the Fourth Amendment (Justice Alito expressly stated this and Justice Sotomayor strongly implied her agreement).

Although the concurring opinions in *Jones* don't directly address the issue, *Karo* may also limit the use of location tracking methods when they reveal a

92. *Id.* at 955-56 (citations omitted).

person's movements within a home or other private areas that are outside of public view.

One final note: Although their decisions are not binding on the United States or California, the Supreme Courts in New Jersey and Massachusetts very recently held that there is a reasonable expectation of privacy in locational data under their state constitutional search and seizure provisions. In those states, non-trespassory location tracking constitutes a "search."[93]

Social Media

The term "social media" is used to describe "forms of electronic communication … through which users create online communities to share information, ideas, personal messages, and other content…."[94] Because social media is typically used to share information widely, it is counter-intuitive that there would be an expectation of privacy with regard to the shared information.

However, it is common for social media to involve closed groups, with access limited to those who have been expressly invited. For example, one could create a Google discussion group to share information with a small group of associates, who must be registered and must enter a password in order to access the information. This seems analogous to a small group of associates meeting out of the public eye to have a private discussion. It is also similar to a telephone conference call involving a small number of participants, or email delivered to a small group of addressees. In this context, it may be reasonable to expect some level of privacy within the group.

Granted, there is no reasonable expectation that any member of a group will preserve the group's confidences. And as a group grows larger in size, the likelihood that the group's "private" communications will be shared with persons outside the group also grows larger. At some point, the size will be such that it is no longer reasonable to expect conversational privacy within the group.

That said, the possibility that a person in a private conversation will breach confidences is not unique to social media. A participant in a face-to-face conversation in one's home or on a two-person telephone call could also share the content of the otherwise private communication. The Court has long

93. See New Jersey v. Earls, 214 N.J. 564 (2013); Commonwealth v. Augustine, 467 Mass. 230 (2014).

94. See <http://www.merriam-webster.com/dictionary/social%20media>.

recognized that possibility and held that a voluntary disclosure of a private conversation is not a search.[95]

The staff found no Supreme Court guidance on this question and sees no easy way to determine, in any particular case, whether a social media user has a reasonable expectation of privacy with regard to shared information. A password protected group of two seems very different from Facebook content that is shared with hundreds of friends (any of whom can republish that content to their own circle of friends, simply by commenting on it). The former could be analogized to a private telephone conversation; the latter to a conversation conducted in the middle of a party.

Ultimately, the question of whether one has a reasonable expectation of privacy in social media content probably varies from case to case, depending on one or more of the following factors:

- *Is membership unrestricted?* Is any person who asks to join the group admitted to membership? If so, then there is likely to be less of an expectation of privacy. By contrast, if membership is restricted to a close circle of confidants, the expectation of privacy is probably greater.
- *How large is the group?* As discussed above, the larger the group the greater the likelihood that confidences will be shared with outsiders.
- *What privacy protections are guaranteed in the user agreement?* If a service provider reserves a broad right to share user information with others, the user's reasonable expectation of privacy would be diminished. Conversely, if a service provider promises strong privacy protection as a feature of the service, then the reasonable expectation of privacy would be strengthened.

The third party doctrine also comes into play. Like all other communication services, social media necessarily involves a third party intermediary who provides the forum for communication. All of the content shared on a social media site is also voluntarily provided to that third party. Under the existing federal third party doctrine, that might be enough to defeat any reasonable expectation of privacy (depending on whether the third party doctrine applies to communicative content).

95. See, e.g., Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

But, as discussed before, the California Constitution is not governed by the third party doctrine. While one expects to share information within a social media group, it is probably not expected that the third party service provider will share that information with outsiders (especially if the service agreement guarantees that this will not be done). Information shared on a social media site may include broad details of a person's private life, sufficient to construct a "current virtual biography." For those reasons, it seems likely that the involvement of a third party intermediary would not preclude the application of the California Constitution to social media content.

But that still leaves the unanswered question, discussed at the outset, of the extent to which one can reasonably expect privacy with regard to information that is shared with a closed group.

Anonymity

One feature that the Internet provides is anonymity. A person can send email or post information to discussion forums using a pseudonym or with no attribution at all. Is there a reasonable expectation of privacy with regard to a person's identity when engaging in anonymous communication on the Internet? If the government requires that a service provider disclose the identity of a customer associated with particular communicative content, is that a "search?"[96]

The staff could find no Supreme Court case directly addressing this issue. However, it seems likely that it would fall under the ambit of the third party doctrine. In order to establish an anonymous presence on the Internet, a customer must provide identifying information to the service provider. Under the third party doctrine, the customer would probably be held to bear the risk that the service provider will disclose that voluntarily provided metadata, defeating any reasonable expectation of privacy as to that data.

The federal circuit courts have generally taken that approach to the issue, applying the third party doctrine to government requests for a customer's account information:

96. The staff anticipates that the protection of customer anonymity will also present constitutional issues relating to free expression, free association, and general privacy (under the California Constitution). Those issues are not discussed here. They will be examined in a future memorandum.

> Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.[97]

It seems likely that this would not be the result under the California Constitution. In *People v. Chapman*,[98] one of the series of California Supreme Court cases holding that the federal third party doctrine does not apply to the California Constitution, the court specifically found a reasonable expectation of privacy in the identity associated with an unlisted telephone number. It seems likely that the court would take the same view of the identity associated with anonymous online content.

However, there is one point on which the two scenarios differ. In *Chapman*, the court stressed that a telephone subscriber must pay an extra fee to have an unlisted telephone number. This implies a greater than usual interest in privacy, supporting the notion that privacy was reasonably expected.[99]

By contrast, there is typically no extra charge or step that must be taken in order to acquire a pseudonym for use on the Internet. Indeed, on popular web services, it is often necessary to choose a pseudonym as a user name, because most common first and last name combinations have already been taken. So the special inference that the *Chapman* court drew from the fact that telephone customers must take extra steps in order to achieve anonymity does not seem applicable to routine Internet anonymity.

That said, many Internet services allow users to establish a public profile to go with a user name. This allows users to present a real identity if they choose to do so. If a person does not disclose a real identity, that might suggest a subjective desire for privacy.

Nonetheless, it seems clear that there are many situations in which Internet anonymity is used to avoid being associated with controversial positions or to protect intimate details about a person's life. For example, the website patientslikeme.com provides an anonymous forum where people with specific illnesses can discuss their treatments, symptoms, and prognosis. This allows users to share useful information and provide emotional support, within the confines of a group where everyone has had similar experiences and challenges. For example, users experiencing clinical depression might discuss their

97. U.S. v. Perrine, 628 F.3d 1196, 1204-05 (2008) (and cases collected therein).
98. 36 Cal. 3d 98 (1984).
99. *Id.* at 108.

experiences with attempted suicide, psychoactive drug treatments, and the failure of personal relationships. Anonymity provides the ability to have such conversations frankly, without concern for the potentially destructive consequences if the information were traced back to the person providing it. The patientslikeme.com site states that it will generally not share a member's name, email address, mailing address, or date of birth with other persons (with expressly stated exceptions, including the possibility of opting in to a public registry).[100] It seems very likely that users who remain anonymous subjectively expect their identities to remain private. Moreover, that expectation seems quite reasonable, as it is a necessary condition for potentially therapeutic social networking.

While there may be many instances in which a person has no subjective expectation of privacy as to that person's identity in the context of anonymous Internet communication, it seems likely that there are many instances where there is such an expectation. If such anonymity is guaranteed by a service provider and serves an important purpose, a court might well find an expectation of privacy as to customer identity is reasonable.

Cloud Computing

"Cloud computing" refers to "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet."[101] Any type of data can be stored on a cloud computing service, including address books, personal or business papers, photographs, and video clips.

Cloud computing services can be configured so as to provide access to a single user only. In this configuration, cloud computing serves the same purpose as a hard drive in a desktop computer or a USB flash drive carried in one's pocket. It simply provides storage for one's electronic data files. However, this storage has the added advantage of being accessible over the Internet, so that the stored data can be accessed or modified from any location that has a net connection (including most modern smartphones).

Cloud computing can also be configured for access by a group of people (who have been registered as users and issued passwords). In this configuration, cloud storage is functionally similar to social media. It presents the same sorts of

100. See < http://www.patientslikeme.com/about/privacy>.
101. See < http://www.merriam-webster.com/dictionary/cloud%20computing>.

questions about reasonable expectations of privacy in group communications. See the discussion of social media, above.

Setting that issue aside, is there a reasonable expectation of privacy with regard to electronic files that are stored on a third party's server? If the government requires that those files be turned over, is this a "search" for constitutional purposes?

Contents of Computer Generally

While the staff could find no decision of the United States Supreme Court directly addressing the application of the Fourth Amendment to files stored on a computer, the federal circuit courts have generally found a reasonable expectation of privacy with regard to the contents of a computer or other electronic storage device:

> When confronted with this issue, courts have analogized the expectation of privacy in a computer to the expectation of privacy in closed containers such as suitcases, footlockers, or briefcases. Because individuals generally retain a reasonable expectation of privacy in the contents of closed containers, see *United States v. Ross*, 456 U.S. 798, 822-23 (1982), they also generally retain a reasonable expectation of privacy in data held within electronic storage devices. Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable expectation of privacy in the information. See *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding reasonable expectation of privacy in a personal computer); *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (same); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."); *United States v. Reyes*, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); *United States v. Lynch*, 908 F. Supp. 284, 287 (D.V.I. 1995) (same); *United States v. Chan*, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same); see also *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) ("A personal computer is often a repository for private information the computer's owner does not intend to share with others. For most people, their computers are their most private spaces." (internal quotation omitted)).[102]

102. U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 3-4 (3d ed. 2009).

Under that line of reasoning, retrieval of files stored on a cloud computing server would seem to be a search. However, the cases discussed above involved files stored on one's own equipment. Would the result be the same if files are stored on a third party's equipment?

Third Party Doctrine

When one stores a file on a cloud computing server, one is voluntarily submitting the file to a third party for a limited purpose. Under the now familiar analysis discussed repeatedly above, this could trigger application of the federal third party doctrine. That could defeat any reasonable expectation of privacy with regard to the Fourth Amendment.

On the other hand, it is not entirely clear that the customer is actually "providing" the content of stored files to a third party service provider in any meaningful sense. There is no need or expectation that the service provider will ever examine the content of the files. Such files are not like a bank's transactional records, where bank officers necessarily examine the records in the ordinary course of business. They seem more like the content of a safe deposit box. Such content is placed into the bank's possession and safekeeping, but it is reasonable to expect that the bank will not open a safe deposit box and examine its contents. Of course, that analogy depends on an assumption that the content will not actually be examined by the service provider.

In any event, the federal third party doctrine has not been applied to the California Constitution. The reasoning of the California Supreme Court on that point would seem to apply to cloud computing. One does not expect a cloud storage provider to share stored content with outsiders, especially if the service agreement guarantees that such sharing will not occur. And there is no limit to the types of private information that could be stored on a cloud server. Such data could easily reveal enough personal information to provide a "current virtual biography."

WARRANT REQUIREMENT

Assuming that a "search" has occurred, what do the Fourth Amendment and the California Constitution require? The search must not be "unreasonable" and any warrant issued must be grounded on probable cause, supported by oath or affirmation, and describe with particularity the place to be searched and the

persons or things to be seized. The main elements of those requirements are summarized briefly below.

Warrant Generally Required

The U.S. and California Constitutions prohibit "unreasonable" searches, but do not expressly require that a warrant be issued. Nonetheless, the courts have generally held that a warrantless search is per se unreasonable:

> The Government urges that, because its agents relied upon the decisions in *Olmstead* and *Goldman*, and because they did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," *Agnello* v. *United States*, 269 U.S. 20, 33, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . ." *Wong Sun* v. *United States*, 371 U.S. 471, 481-482. "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," *United States* v. *Jeffers*, 342 U.S. 48, 51, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment -- subject only to a few specifically established and well-delineated exceptions.[103]

Exceptions to the warrant requirement that may be relevant to electronic communications are discussed further below.

Probable Cause

A search warrant may only be issued on a showing of probable cause, supported by oath or affirmation.

---

103. *Katz*, 389 U.S. at 356-57 (footnotes omitted).

> Probable cause under the Fourth Amendment exists where the facts and circumstances within the affiant's knowledge, and of which he has reasonably trustworthy information, are sufficient unto themselves to warrant a man of reasonable caution to believe that an offense has been or is being committed.[104]

Said another way:

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a "substantial basis for . . . [concluding]" that probable cause existed.[105]

The federal probable cause standard has been applied by California courts, without any indication that a different standard might apply to the California Constitution.[106]

Particularity

The search and seizure provisions of the US and California Constitutions expressly require that a warrant "particularly [describe] the place to be searched and the persons and things to be seized." This particularity requirement was a response to the "general warrants" that had been used by England in colonial times, which have been identified as one of the grievances that had prompted the Declaration of Independence:

> The use of [general warrants] was a motivating factor behind the Declaration of Independence. In view of the many cases commenting on the practice it is sufficient here to point out that under these "general warrants" customs officials were given blanket authority to conduct general searches for goods imported to the Colonies in violation of the tax laws of the Crown. The Fourth Amendment's requirement that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized," repudiated these general warrants and "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is

104. Berger v. New York, 388 U.S. 41, 56 (1967).
105. Illinois v. Gates, 462 U.S. 213, 238-39 (1983).
106. See, e.g., People v. Scott, 52 Cal. 4th 452, 474 (2011); Wood v. Emmerson, 155 Cal. App. 4th 1506, 1519, 66 Cal. Rptr. 3d 847 (2007).

> left to the discretion of the officer executing the warrant." *Marron* v. *United States*, 275 U.S. 192, 196 (1927)….[107]

The Department of Justice describes the particularity requirement as follows:

> The Fourth Amendment requires that every warrant "particularly describ[e]" two things: "the place to be searched" and "the persons or things to be seized." U.S. Const. Amend. IV; see *United States v. Grubbs*, 547 U.S.90, 97 (2006). Describing with particularity the "things to be seized" has two distinct elements. See *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999). First, the warrant must describe the things to be seized with sufficiently precise language so that it tells the officers how to separate the items properly subject to seizure from irrelevant items. See *Marron v. United States*, 275 U.S.192, 296 (1927) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); *Davis v. Gracey*, 111 F.3d 1472, 1478 (10th Cir. 1997). Second, the description of the things to be seized should be limited to the scope of the probable cause established in the warrant. See *In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853,857 (9th Cir. 1997). Considered together, the elements forbid agents from obtaining "general warrants" and instead require agents to conduct narrow seizures that attempt to "minimize[] unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).[108]

The California Supreme Court has concluded that the Fourth Amendment's particularity requirements are identical to those of the California Constitution:

> The relevant language of article I, Section 13 of the California Constitution parallels the relevant language of the Fourth Amendment, and "the issue of particularity resolves itself identically under both federal and California standards."[109]

Notice

In *Berger v. New York*, the Supreme Court held that a court order authorizing a wiretap pursuant to a New York statute violated the Fourth Amendment in a number of ways.[110] One of the constitutional deficiencies of the wiretap statute was that it authorized the issuance of a warrant without notice to the target of the wiretap, and without any showing of exigent circumstances to justify the lack of notice:

---

107. *Berger*, 388 U.S. at 58.
108. U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 69 (3d ed. 2009).
109. People v. Robinson, 47 Cal. 4th 1104, 1132 (2010).
110. Berger v. New York, 388 U.S. 41 (1967).

> Finally, the statute's procedure, necessarily because its success depends on secrecy, has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts. On the contrary, it permits unconsented entry without any showing of exigent circumstances. 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.[111]

Shortly after *Berger* was decided, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act.[112] "Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967)."[113]

Title III requires that notice of a wiretap be given to persons named in the warrant (and others at the judge's discretion) within a "reasonable time" (but no later than 90 days) after expiration of the warrant authorizing a wire interception.[114] This notice may be postponed on an ex parte showing of good cause.[115] The staff did not find any case holding that provision constitutionally insufficient.

Relevant Warrant Exceptions

There are a number of established exceptions to the presumptive requirement of a warrant to conduct a reasonable search under the Fourth Amendment. Many are not discussed below because they would not involve customer information provided by a communication service provider (e.g., a vehicle search, search incident to lawful arrest, search of items in "plain view" or "open fields," booking inventory search, or border search).

A few exceptions that could be relevant to the current study are discussed briefly below.

Consent

No warrant is required to conduct a search if a person with authority voluntarily consents to the search.[116] For example, a customer could voluntarily

111. *Id*. at 60.
112. 18 U. S. C. §§ 2510-2520.
113. United States v. United States Dist. Ct., 407 U.S. 297, 302 (1972).
114. 18 U.S.C. 2518(8)(d).
115. *Id*.
116. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

consent to government access to his or her own records held by a communication service provider. No warrant would be required.

Similarly, if two or more people share an email account (or other Internet-based service account), any of those persons might have sufficient control to consent to a search of the related content:

> The authority which justifies the third-party consent does not rest upon the law of property … but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right, and that the others have assumed the risk that one of their number might permit the common area to be searched.[117]

Although that case involved a search of real property, the same principle could be applied to shared access to virtual "common area."

By extension, it may also be true that a social networking participant could consent to a search of the information available to all members of the group. In such a situation, the participants might have mutual use and joint access sufficient to provide authority to consent to the search. Moreover, as discussed earlier, one always bears the risk that another person involved in a communication will be a police agent or voluntarily share information with the police.[118]

Finally, it is possible that a service agreement might allow the service provider to exercise such a high degree of control over customer data, that the service provider would have sufficient joint control to authorize a search. For example, in *United States v. Young*,[119] the Sixth Circuit found that Federal Express could consent to a warrantless government search of a customer's packages because Federal Express had expressly informed its customers that it reserved the right to open and inspect any package for any reason:

> Courts have recognized that a third party has actual authority to consent to a search of a container if the owner of the container has expressly authorized the third party to give consent, or if the third party has mutual use of the container and joint access to or control over the container. *See, e.g., United States v. Fultz*, 146 F.3d 1102,

117. United States v. Matlock, 415 U.S. 164 (1974).
118. See, e.g., Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").
119. 350 F.3d 1302 (2003).

> 1105 (9th Cir.1998). We see no reason why this concept should not extend to packages shipped through private carriers when those carriers have explicitly warned those utilizing their services that their packages are subject to search.[120]

On a related but slightly different point, if a third party service provider conducts its own search of customer information, on its own initiative, discovers evidence of a crime, and then turns the information over to the government, this private action would probably not be a search under the Fourth Amendment. For example, in *United States v. Jacobsen*,[121] employees of a private freight carrier inspected a damaged package and discovered that it contained a white powder. They contacted the Drug Enforcement Agency who assayed the powder, found it to be cocaine, and initiated an investigation. Although the sender had a reasonable expectation of privacy, the Fourth Amendment does not apply to this type of private search:

> The initial invasions of respondents' package were occasioned by private action. Those invasions revealed that the package contained only one significant item, a suspicious looking tape tube. Cutting the end of the tube and extracting its contents revealed a suspicious looking plastic bag of white powder. Whether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character.
>
> The additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search.[122]

Parole and Probation

A person may be subject to warrantless search as a condition of parole or probation. The Court upheld such a condition against a Fourth Amendment challenge in *Griffin v. Wisconsin*,[123] reasoning that a parolee has a reduced expectation of privacy.

Such an exception could be relevant to this study. For example, many sex offenders are subject to parole or probation conditions that limit their use of the Internet. A government request for customer information for the purpose of determining whether the customer has violated such a condition could fall within the scope of this exception.

120. *Id.* at 1308.
121. 466 U.S. 109 (1984).
122. *Id.* at 115.
123. 483 U.S. 868 (1987).

Exigent Circumstances

A warrantless search can sometimes be justified where there is probable cause and exigent circumstances require immediate action. For example, an immediate search might be required to protect safety or prevent the destruction of evidence.[124] One can imagine scenarios in which exigent circumstances might justify a warrantless search of customer records held by a communication service provider (e.g., an immediate request for location tracking of a person where there is probable cause to believe the person has abducted a child and is in flight).

SUMMARY

As discussed above, there is very little Supreme Court case law directly addressing the application of the Fourth Amendment to the sorts of communication technologies at issue in this study. This is partly because those technologies are so new. There has not been sufficient time for many relevant cases to work their way up to the Supreme Court. It is partly because the need to litigate the scope of the Fourth Amendment in this area has been largely obviated by federal statutory law, which covers much of the same ground. Finally, the Supreme Court has indicated its reluctance to litigate these issues, expressly signaling that the complex of issues should be handled by Congress. They may also be waiting for fuller development of the issues in the lower courts.

The fact that suppression of evidence is unavailable as a remedy for violations of the California Constitution means that there is little incentive for criminal defendants to assert a violation of Section 13 of Article 1. This has undoubtedly slowed the development of case law addressing the application of the California Constitution to these types of new communication technologies.

Consequently, the analysis in this memorandum is grounded largely on extrapolation from principles established in other contexts. In some cases, fairly close analogies can be drawn (e.g., the principles on government access to telephone metadata seem readily applicable to Internet metadata). In other cases, analogies are harder to find (e.g., social media).

The conclusions drawn in the discussions above are summarized very briefly below.

---

124. See, e.g., Warden v. Hayden, 387 U.S. 294 (1967) ("The Fourth Amendment does not require officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others."); see also Georgia v. Randolph, 547 U.S. 103, 117 n.6 (U.S. 2006) (collecting cases).

Wiretaps and Bugs. There is a reasonable expectation of privacy with respect to the content of landline telephone calls. Interception of the content of calls is a search for constitutional purposes. The same is true of the use of electronic listening devices to eavesdrop on private conversations.

Cell Phones and Internet Audio and Visual Conversation. Although the staff found no Supreme Court decision directly on point, it seems likely that there is a reasonable expectation of privacy in the content of cell phone calls and Internet-based audio and visual communications. That said, the reasonable expectation of privacy could be defeated if using a device that relies on an easily intercepted transmission medium.

Text-Based Electronic Communications. The staff found no Supreme Court case deciding whether the interception or retrieval of email or other text-based electronic communications would be a search for constitutional purposes (in fact, the U.S. Supreme Court has expressed its "disinclination" to decide such issues). The only federal appellate court to decide the question found that there is a reasonable expectation of privacy in the content of email. That court analogized email to both a telephone call (which is generally protected by the Fourth Amendment) and to regular mail (in which there is a reasonable expectation of privacy until delivered). The court attempted to distinguish email from the cases holding that there is no reasonable expectation of privacy in information voluntarily provided to a third party for a limited purpose, by pointing out that the third party (the ISP) acts only as an intermediary, rather than the recipient of the information. Although the staff is unsure whether that argument would prevail in the Supreme Court, it is probably irrelevant in California. The third party doctrine has not been applied to the California Constitution.

Metadata. The Supreme Court has held that there is no reasonable expectation of privacy in telephone metadata. The same principle would seem to apply to Internet metadata (e.g., email addresses of messages sent and received). And, in fact, the federal appellate courts have repeatedly held that to be the case. Under the California Constitution, there is a reasonable expectation of privacy as to telephone metadata. The staff sees no reason why the same would not be true of Internet metadata.

Social Media. The staff found no Supreme Court case deciding whether there is a reasonable expectation of privacy in information shared in closed Internet

discussion groups. It seems likely that the reasonableness of any expectation of privacy would depend on the size of the group and the strictures in place to preserve privacy. Under the Fourth Amendment, the third party doctrine would come into play and might be sufficient to defeat the reasonable expectation of privacy in many cases. That would not be an issue under the California Constitution. *It seems likely that constitutional guarantees of freedom of expression, association, and general privacy will also be relevant to the protection of social media content. That will be discussed in future memoranda.*

Location Data. The staff found no Supreme Court case deciding whether non-trespassory location tracking (i.e., cell tower triangulation or mobile device GPS tracking) is a search for constitutional purposes. That said, in *U.S. v. Jones*, all five of the concurring justices indicated that such tracking would be a search in some circumstances (including under the facts before the court, four weeks of tracking the location of a car used by a suspected drug trafficker). According to the four justices who joined in the concurrence authored by Justice Alito, the deciding factor is the duration of the tracking and the seriousness of the suspected crime. This seems to reflect the notion that there is no reasonable expectation of privacy in your location if it would have been practicable for police to track you using traditional methods. If location tracking lasts longer than would have been practicable given the seriousness of the suspected offense, then there is a reasonable expectation of privacy. Moreover, under *Karo*, any tracking that reveals the target's location within private spaces, where public tracking would not have been possible, may constitute a search. While it is not possible to determine exactly what facts would trigger the application of the Fourth Amendment, it seems very likely that it does apply in many situations. Thus, a statute that allows location tracking without a warrant could be unconstitutional as applied in some cases.

Anonymity. The staff found no Supreme Court case deciding whether a government demand for the identity of a person associated with anonymous Internet content would be a search. Under the third party doctrine, it would probably not be a search, and many circuit courts have so held. This is especially likely because the information at issue is metadata, rather than communicative content. However, the third party doctrine would probably not defeat the reasonable expectation of privacy under the California Constitution. This seems especially likely given the strongly analogous decision in *Chapman*, which found

a reasonable expectation of privacy in the identity associated with an unlisted telephone number.

Cloud Computing. The staff found no Supreme Court case deciding whether a government demand for files stored on a cloud computing service would be a search. In general, there can be a reasonable expectation of privacy with regard to files stored on a computer in one's own possession. But when files are stored on a third party's equipment, the situation becomes more complicated. The federal third party doctrine might defeat any reasonable expectation of privacy. However, as discussed above, in cases where the provider is not expected (or authorized) to access stored content, the doctrine may not apply. Moreover, the third party doctrine would probably not apply under the California Constitution.

Exceptions to Warrant Requirement. The most significant exception to the requirement of a warrant arises when a person with authority voluntarily authorizes a search. There may be circumstances in which a service provider reserves the right to access content to such a degree that the provider might have authority to consent. Moreover, the Fourth Amendment would not be implicated if the service provider conducted its own private search and then related its findings to the government. These considerations are heavily dependent on the extent to which a service provider retains authority to access content, which likely varies from company to company. Exceptions for exigent circumstances and probation or parole conditions are also likely to be relevant.

Respectfully submitted,

Brian Hebert
Executive Director