Privacy in the Cell Phone Age: New Restrictions on Police Activity

Michael D. Ricciuti*

“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”

I. INTRODUCTION

Five decades ago, in Katz v. United States, Justice Harlan expressed his understanding of the scope of Fourth Amendment protection:

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.

In part based on Katz, the Supreme Court established a body of Fourth Amendment law, including what became known as the “third-party doctrine.” The third-party doctrine provides that a citizen is not entitled to Fourth Amendment protection for information or documents he or she entrusts to a third party—say checks negotiated through a bank or a telephone service numbers

* Mr. Ricciuti is a graduate of Harvard Law School and a member of the adjunct faculty at Suffolk University Law School. While he serves as an Associate Justice of the Superior Court of Massachusetts, this Article is not written in the name of the court and the views expressed here are his own. Further, this Article focuses on federal law rather than on Massachusetts state law. Mr. Ricciuti expresses his deep appreciation to the staff of the Suffolk Law Review for the opportunity to speak at its Internet of Things symposium. This Article is based on that speech.

3. Id. at 361 (Harlan, J., concurring).
dialed using a telephone company’s services—because there is no legitimate privacy interest in the documents or information that were voluntarily shared with the third party. Applying this doctrine was challenging prior to the advent of technologies that permitted citizens to entrust large swaths of their private information to servers operated by third parties. After the digital revolution, it became more than challenging, as Justice Sotomayor noted in the quote above.4

This Article focuses on this issue and on the developing principles in criminal cases governing search and seizure of digital evidence maintained on or created using cell phones. The Supreme Court has been grappling with the scope of Fourth Amendment protection over such digital evidence in earnest since 2012, and it has rendered three significant, privacy-protective decisions. In them, the Supreme Court has rejected a blanket application of the third-party doctrine, but has not abandoned the concept either.

The net result is unclear. At its core, the issue in these cases is consent—when do citizens consent to a waiver of their privacy when they use third-party mechanisms to store information or communicate with one another, and how far does such consent extend? Whether and how a citizen’s “assumption of the risk” of disclosure plays in this analysis is open to question, and it is unclear how a court should decide whether and to what extent a waiver of privacy rights has been made. One of the new cases permits a potentially powerful argument that police action, as opposed to action by others, is subject to greater restriction than action by private citizens, so that digital privacy is protected from the government’s scrutiny but not from the scrutiny of at least some ordinary citizens. But how far that protection extends is also subject to serious question. Moreover, even where the Court does not find a broad waiver of privacy, especially against police surveillance, and requires issuance of search warrants, before such information can be obtained by the police, the reality in the new digital world is that users are increasingly creating and voluntarily sharing data more freely and more broadly that has been the case historically, even extremely private data like DNA profiles. The real questions posed by these cases, then, is not only whether the Court will extend privacy protections despite this sharing and, but also whether it will matter.

II. OVERVIEW

As is well known today, cell phones are not just telephones. They are not even primarily telephones. They are powerful computers with built-in, automatic, and (often) unnoticed tracking devices.5 And they are ubiquitous; it

---

4. See supra note 3 and accompanying text (identifying Justice Sotomayor’s concerns with the third-party doctrine).
5. Riley v. California, 573 U.S. 373, 393 (2014) (comparing cell phones to computers because of elaborate capabilities).
is virtually impossible to survive in modern society without one.\textsuperscript{6} As a consequence, virtually all citizens carry a computer capable of storing massive amounts of personal data and permitting instantaneous global communication—while simultaneously and incidentally serving as a personal global positioning system (GPS) device.\textsuperscript{7}

Over the past handful of terms, the Supreme Court has wrestled with whether police must obtain search warrants to access information stored on these devices or held by the communication companies that provide them with cellular services.\textsuperscript{8} Well-established case law suggested that no search warrant was necessary to seize what was on the phone or stored with the cell phone companies supporting it.\textsuperscript{9} Further, at arrest, the law had long permitted the police to seize and search things found on a defendant’s person, which would include cell phones.\textsuperscript{10} For the same reason that a search of the defendant’s wallet upon arrest was permissible, the police argued that so was the search of his or her cell phone. And if information generated using the cell phone was stored with a third party, the third-party doctrine—a concept based on cases decided in the 1970s—held that the evidence was available to government agents armed with no more than a subpoena because the information had already been disclosed to a third party and was therefore no longer private and protected against disclosure to the police under the Fourth Amendment.\textsuperscript{11}

Applied blindly, then, case law developed for a different era threatened the privacy over everything on a cell phone or communicated using it, regardless of how much personal data, was put at risk of disclosure. In addition, data generated by the cell phone company itself—which is neither created by the user nor accessed by him or her—might also be available to the government just for the asking. Would it matter whether the user were unaware that such information was created in the first place? What if the information captured provided a

\textsuperscript{6} Carpenter, 138 S. Ct. at 2211. “There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.” \textit{Id.}

\textsuperscript{7} See \textit{id.}

\textsuperscript{8} See, e.g., \textit{id.} (presenting question of whether access to cell phone records constitutes government search); \textit{Riley}, 573 U.S. at 378 (opining whether police may search cell phone data of arrestees without warrant).

\textsuperscript{9} See United States v. Miller, 425 U.S. 435, 443 (1976); see also Smith v. Maryland, 442 U.S. 735, 741-42 (1979); infra Section III.B (discussing \textit{Miller} and \textit{Smith} in detail).

\textsuperscript{10} United States v. Robinson, 414 U.S. 218, 233-34 (1973) (finding search of person incident to his arrest lawful).

\textsuperscript{11} See infra Section III.B.
detailed, historical record of everywhere the user went with the phone? Was that data private at all?

Three recent decisions addressed these questions, at least in part. First, the GPS case, *United States v. Jones*,12 concerned whether the government could attach a GPS device and track a vehicle’s movements without a warrant.13 Second, the cell phone case, *Riley v. California*,14 decided in 2013, examined whether the search incident to arrest exception to the warrant requirement allowed the police to search the data maintained in a cell phone seized from a defendant at arrest, including data held by third parties.15 Third, and most importantly, *Carpenter v. United States*,16 decided in mid-2018, analyzed whether the third-party doctrine applied to permit the police to obtain without warrant location information generated automatically by a cell phone service provider, which effectively tracked the location of a cell phone the entire time it was turned on.17

In each of these cases, the Court re-interpreted well-established law to restrict the ability of the police to search electronic information without a warrant, albeit they did so somewhat inconsistently.18 These decisions were rights-protective, and may well spell the doom of the third-party doctrine, one of the historically powerful arguments relied upon by the government to justify seizure of records held on behalf of individuals by others. But any conclusion that these cases put to rest the risk to privacy in the digital world would be seriously mistaken.

III. THE FOURTH AMENDMENT, PRIVACY AND THE THIRD-PARTY DOCTRINE

A. Privacy Under the Fourth Amendment

The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated.”19 For generations, the key test for determining what is private and therefore within the scope of the Fourth Amendment was articulated in *Katz*.20 Interestingly, the *Katz* test was not found in the majority opinion in that case, but was set out in Justice Harlan’s well-known

13. Id. at 402 (introducing question presented).
15. Id. at 378 (opining whether arrest permits warrantless search of cell phone).
17. Id. at 2211 (opining validity of cell phone record search leading to information on individual’s movements).
18. See United States v. Jones, 565 U.S. 400, 405-06 (2012) (noting variance among cases on point); see also *Carpenter*, 138 S. Ct. at 2220-21 (analyzing prominent Supreme Court cases to reach decision); *Riley*, 573 U.S. at 403 (acknowledging impact to come from decision).
19. U.S. CONST. amend. IV.
In Harlan's concurrence, a two-pronged definition of what is private and therefore within the scope of the protection of the Fourth Amendment, a definition which guided Fourth Amendment jurisprudence ever since: “My understanding of the rule that has emerged from prior decisions is that there is a two-fold 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.” If both of these requirements are met—that the rights-holder has a subjective expectation of privacy, and that society, objectively, recognizes the expectation as reasonable—the interest is protected under the Fourth Amendment. Embedded in this definition is the concept of waiver—that a claimant to an expectation of privacy and society’s assessment of its reasonableness are subject to intentional or unintentional waiver by the rights holder. Justice Harlan made this point in the next line of his concurrence:

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 the 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.

Under this definition, then, a person who keeps private matters in a protected place, like a home, could still forfeit the privacy protection over that matter if he or she removes the private matter from the protected place and thereby exposes it to “outsiders.” Even if the rights-holder believes his private matter is private, he may still forfeit the Fourth Amendment’s protections if he conducts his private business in a non-private place. In either event, the right holder’s expectation of privacy may become untenable, or society will not recognize the privacy claim as reasonable, or both. In that case, there would be no protectable Fourth Amendment interest, and hence no search if the information is obtained by the government and no need for the government to obtain a search warrant to do so.

B. The Third-Party Doctrine

These limitations on privacy played out in the 1970s to limit the scope of interests protected by the Fourth Amendment. In the analog world, there were questions about just how a person successfully kept private matters from the view of outsiders. In two cases, the government successfully argued that the fact that third parties held putatively private information could undermine an expectation

21. Id. at 361 (Harlan, J., concurring).
22. Id.
23. Id.
of privacy and make a search warrant unnecessary. What developed became known as the third-party doctrine.

United States v. Miller, decided in 1976, involved a suppression motion directed at records maintained by a bank—microfilmed copies of checks, deposit slips and the like—which the government had subpoenaed. Miller argued that the records were improperly seized. The appeals court agreed. It “assumed that [Miller] had the necessary Fourth Amendment interest” to find that the government’s seizure of the documents amounted to “compulsory production of a man’s private papers to establish a criminal charge against him” and that the government had not used a search warrant but rather relied on a subpoena, an inadequate “legal process.” In essence, the appeals court found that the depositor had not lost his privacy protections simply because he maintained his private papers with the bank and that the government had improperly invaded his privacy by seeking records from the bank without a search warrant.

The Supreme Court reversed and found that “there was no intrusion into any area in which [Miller] had a protected Fourth Amendment interest.” In the first place, the Court found that the records were business records of the bank itself, and not private papers of the depositor at all. In the second place, even granting that a federal statute, the Bank Secrecy Act, provided some measure of privacy protection over the records at issue, the Court rejected the depositor’s argument that he had a reasonable expectation of privacy over his supposedly private papers while they were in the hands of the bank. Relying on Katz for the proposition that “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,” the Court found there was no reasonable expectation of privacy over negotiable instruments which were to be used in commercial transactions, or in financial statements and deposit slips, all of which “contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” Thus, “the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government,” and:

---

26. See id. at 436-37.
27. Id. at 438-39.
28. Id. at 440.
29. Miller, 425 U.S. at 443 (quoting Boyd v. United States, 116 U.S. 616, 622 (1886)).
30. Id. at 439.
31. See United States v. Miller, 500 F.2d 751, 756 (5th Cir. 1974).
33. See id. at 440-41.
34. Id. at 442.
35. Id. (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
36. See Miller, 425 U.S. at 442.
37. Id. at 443.
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.\footnote{United States v. Miller, 425 U.S. 435, 443 (1976).}

Because those third parties had access to bank documents like checks, the government did not have to get a search warrant to obtain the records, but could instead rely on a subpoena to obtain them from the bank.\footnote{Id. at 444-46.}

The concept of an “assumption of the risk,” wherein a citizen assumes the risk that a third-party, here a bank, might disclose the citizen’s supposedly private papers, is a powerful argument for the government, more so now that more data is entrusted to third parties than was the case in the 1970s. Viewed in light of today’s digital life, the breadth of that idea and the privacy waiver it entails should be concerning; simply substitute the identity of the information holder, the bank in \textit{Miller}, for a contemporary digital company, say Google, Facebook or SnapChat, to name a few, to get a sense of the breadth of the potential waiver. The parallel is not complete—\textit{Miller} dealt with negotiable instruments (like checks) whose very purpose was to be shared with others—which may distinguish them from those electronic communications that were meant to be private. Others, however, like Facebook posts and the like, are not intended to be confidential, a distinction that may make a difference.\footnote{See infra Part V.}

Shortly after it decided \textit{Miller}, the Court dealt with the trickier situation of telephones in \textit{Smith v. Maryland}.\footnote{442 U.S. 735 (1979).} In that case, the government had installed, without a warrant, a pen register on the Smith’s phone.\footnote{See id. at 737.} A pen register is a device that records the numbers dialed on a telephone, but does not intercept the communications themselves. Back in the days before text messaging was conducted with telephones, the dialed telephone number was simply that, a telephone number divorced from the content of the communications that followed after the telephones were connected.\footnote{See id. at 741. The Court looked to a contemporaneous cases to aid in its determination:}

\begin{quote}
[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.
\end{quote}

was whether a telephone user had a legitimate expectation of privacy regarding the numbers dialed using his or her phone.44

The Court held that the telephone user had no such legitimate expectation of privacy in the dialed numbers.45 Relying on Katz and on Harlan’s concurrence, the Court found that the pen register did not violate a legitimate expectation of privacy.46 As to the first prong of Harlan’s analysis, the Court found it doubtful that telephone users expected privacy in dialed numbers, since those numbers were conveyed to the telephone company which had the ability to record those numbers and use the resulting data—and perhaps use pen registers themselves to identify unwanted callers, a common service offered by telephone companies in the past.47 Thus, for the Court, “it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”48

This was the case even if the calls were made from inside a user’s home, the area subject to the highest Fourth Amendment protection.49 While Smith’s conduct, including calling from home, may have been calculated to preserve the privacy of the contents of the communication conducted using the telephone, it did not protect the privacy of the number dialed because, by necessity, that information had to be conveyed to the telephone company for the communication to occur at all.50 And in any event, under the second prong of Harlan’s analysis, the Court turned held that society would not recognize any such subjective expectation of privacy in the dialed telephone numbers as reasonable because a telephone user voluntarily turned over the called number data to the phone company—a third party—relying on Miller.51 The telephone user, like the bank patron in Miller, assumed the risk of disclosure by that third party to the government.52

Smith argued that the telephone company did not record or bill for local calls like those at issue, and that he thus enjoyed a legitimate expectation of privacy in such locally-dialed telephone numbers.53 The Court rejected that claim, finding that “[t]he fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference” because the caller voluntarily conveyed the numbers to the company and assumed the risk they would be recorded by the company, and the Court saw no reason for the analysis to turn

44. See Smith, 442 U.S. at 737-42.
45. See id. at 742.
46. See id.
48. Id. at 743.
49. See id. at 743.
50. See id. at 743.
51. See Smith, 442 U.S. at 743-44.
52. See id. at 744-45.
“on how the telephone company chose” to bill its customers. In language that resonates in our time, the Court refused to “make a crazy quit of the Fourth Amendment [whereby] . . . the pattern of protection would be dictated by the billings practices of a private corporation.” In the end, the government could access the dialed numbers without a search warrant because there was no expectation of privacy governing data like these which are shared with a third party. The user, after all, had assumed the risk of disclosure.

IV. THE RECENT DECISIONS

It was against the backdrop of these cases that the Court decided Jones, Riley, and Carpenter.

A. United States v. Jones

In 2012, the Court addressed the warrantless attachment of a GPS device to the underside of a vehicle, which the government monitored for almost a month. The question was whether the attachment and monitoring of the device violated the Fourth Amendment.

The Court held that it did, but did not decide the case on Katz grounds—that the owner of the car held a legitimate expectation of privacy in the underside of his car or in the travel of the car on the public roads. Instead, Justice Scalia resurrected an old idea—that the government trespassed on Jones’s property rights in the car. These rights were still also protected under the Fourth Amendment independently from the Katz analysis, finding that “the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.” Specifically, by attaching the GPS device to the owner’s car, the government had physically intruded on an “effect,” the car, and thereby violated the Fourth Amendment. In essence, Jones supplemented the Katz test by recognizing that the Fourth Amendment also prohibited the government from committing a trespass into private property.

Justice Sotomayor concurred in the result, agreeing that, at a minimum, a search occurs within the meaning of the Fourth Amendment when the government obtained information by intruding on a constitutionally protected area. She further noted, however, that the use of a GPS was particularly intrusive: “GPS monitoring generates a precise, comprehensive record of a

\[54. \text{See id.}\]
\[55. \text{Id.}\]
\[56. \text{See supra Part III.}\]
\[57. \text{United States v. Jones, 565 U.S. 400, 402-03 (2012)}\]
\[58. \text{Id. at 402.}\]
\[59. \text{See id. at 406-07.}\]
\[60. \text{Id. at 409.}\]
\[61. \text{See Jones, 565 U.S. at 404.}\]
\[62. \text{See id. at 413 (Sotomayor, J., concurring).}\]
person’s public movements that reflects a wealth of detail about his familial, political, professional, religious, and sexual associations."63 Moreover, the reach and effectiveness of this data gathering and use by the police was concerning:

The Government can store such records and efficiently mine them for information for years into the future. And because GPS 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.64

In light of this new power, Sotomayor questioned whether the Katz test should be revisited: “whether people reasonably expect their movements will be recorded and aggregated in a manner that enable the [g]overnment to ascertain, more or less at will their political and religious beliefs, sexual habits[,] and so on."65 But Sotomayor went further, asking whether the third-party doctrine under Smith and Miller still made sense:

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. 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 [g]overnment 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.

Resolution of these difficult questions in this case is unnecessary, however

64. Id. at 415-16 (citation omitted).
65. Id. at 416.
66. Id. at 417-18 (emphasis added) (citations omitted).
While the Court did not reach the merits of the third-party doctrine, Sotomayor challenged the notion that the scope of privacy protection provided under the Constitution over information should be determined simply by a third parties’ access to such information.67 The Court would address this concern in two cases decided shortly thereafter—Riley and Carpenter.

B. Riley v. California

Riley posed the question whether or not the police could search the contents of a cell phone seized after an arrest as part of a search incident to arrest. The authority of the police to conduct a warrantless search incident to arrest was a long-standing exception to the Fourth Amendment. The Supreme Court recognized in United States v. Robinson68 that in the case of a lawful custodial arrest, a full search of the person was not only an exception to the warrant requirement of the Fourth Amendment, but is also a “reasonable” search:

A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a ‘reasonable’ search under that Amendment.69

As a result, any evidence found on an individual’s person (and of the area within that individual’s reach) in a post-arrest search was subject to seizure, whether it constituted contraband, a weapon, or evidence of the crime.70 The reason for this exception was two-fold: first, to prevent the defendant from using a concealed weapon against the police, the core justification for permitting frisks under Terry v. Ohio;71 and second, to preserve any evidence the suspect might otherwise destroy, a justification not found in Terry.72 As a result, the cigarette

67. See Jones, 565 U.S. at 417-18 (Sotomayor, J., concurring). “[P]hone-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.” See id. at 429 (Alito, J., concurring) In addition, Justice Alito in his concurrence noted that in the future, the notion of what a citizen could expect to remain private, and therefore subject to Fourth Amendment protection under Katz, would have to be understood in light of the increasing availability of GPS tracking data. See id. at 422-23.
69. See id. at 235.
70. See id. at 224 (highlighting ability to search person and area within immediate control following valid arrest).
71. 392 U.S. 1 (1968).
package seized in Robinson—hardly a weapon—could be seized for purely evidentiary purposes.\textsuperscript{73}

The issue in Riley was “whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.”\textsuperscript{74} Riley consolidated two cases, each involving an arrest in which government agents reviewed the contents of a cell phone found with the defendant. They did so under the authority of Robinson: that because the government could search containers found on arrestees without a warrant, cell phones seized were nothing more than high-tech containers.\textsuperscript{75} Chief Justice Roberts, writing for the Court, rejected this reasoning based on the nature of the privacy right at issue: “Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson."\textsuperscript{76} The government’s seizure of the cell phone itself was one thing—such a seizure was authorized under Robinson to protect that piece of evidence from destruction. But the search of its contents was not supported by that thinking\textsuperscript{77} and, unlike the search of the cigarette package in Robinson, permitting such a search imposed a quantitatively and qualitatively greater intrusion on individual privacy.\textsuperscript{78}

As Roberts wrote, “[a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement ‘by assessing . . . the degree to which it intrudes upon an individual’s privacy and . . . which it is needed for the promotion of legitimate governmental interests.’”\textsuperscript{79} He recognized that cell phones are not like a wallets, which hold a limited amount of information; instead, they are mini-computers, which hold a

\textsuperscript{73} See Robinson, 414 U.S. at 234-236.

\textsuperscript{74} See Riley v. California, 573 U.S. 373, 378 (2014).

\textsuperscript{75} See id. at 379. The Court noted that “[t]he detective testified that he ‘went through’ Riley’s phone ‘looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns,’” illustrating his intent to find evidence when looking through the phone. Id.

\textsuperscript{76} See id. at 386.

\textsuperscript{77} See id. at 386 (declining to extend Robinson to search of cell phone data).

\textsuperscript{78} See Riley, 573 U.S. at 393-98 (highlighting differences between cell phones and other objects traditionally found on arrestees’ person).

\textsuperscript{79} Id. at 385-86.
wide variety of data in significant quantity. 80 This was something new—"[b]efore cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read."81 Indeed:

First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception . . . . [I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.82

Echoing Sotomayor in Jones, Roberts also recognized that, qualitatively, a cell phone would give the government more information than the police could realistically historically gather investigatively—records of internet searches, detailed historical GPS information, information contained in mobile applications (apps) that showed personal interests, and detailed records of the substance of communications.83 Thus, searching a cell phone was not the same as searching his pockets at arrest, Roberts found—it was more akin to allowing the police to ransack a suspect’s house, and then some.84 Moreover, the data to which the government would have access with a cell phone is not limited to what existed on the phone, but would possibly extend to information stored remotely.

81. See id. at 393-94.
82. See id. at 394-95 (citations omitted).
83. See id. at 395-96.
84. See Riley, 573 U.S. at 396-97.
and accessible using the phone. Allowing a search to reach this information “would be like finding a key in a suspect’s pocket and arguing that it allowed law enforcement to unlock and search a house,” especially because officers looking through cell phone data may not be able to tell whether the information “was stored locally at the time of the arrest or has been pulled from the cloud,” that is, stored remotely.

*Riley* avoided the third party issue—it focused on data that was found on the phone itself, and the government conceded that retrieving files from the cloud would go beyond a search incident to arrest. But in a sense, *Riley* turned the third party argument on its head, at least in dicta: It did not find that the fact that data was held by third parties constituted a *waiver* of privacy, but rather found that the ability of cell phones to *access* data that had been shared with third party providers was one reason to *preserve* the privacy of data contained in a cell phone from search. Even so, *Riley* left open the possibility that, while police could not use a phone seized at arrest to access information stored in the cloud, they may seize such information from the service provider without a warrant on the theory that the cell phone user conveyed the data to the provider, much as Smith conveyed the telephone numbers to the telephone company.

**C. Carpenter v. United States**

The third-party doctrine was further weakened, and perhaps frozen in its current position, when the Court decided *Carpenter* in June, 2018. In *Carpenter*, the Court looked at whether the government could obtain, without a warrant, information generated by cell phone companies, known as cell-site location information (CSLI), which effectively tracks the movement of a cell phone while it is on. CSLI is, in essence, increasingly precise, personal GPS data: Whenever a cell phone is on, it communicates with the nearest cell tower. Cell companies keep time-stamped data on which cell tower is nearest the phone. By tracking the cell towers communicating with the cell phone, the government can recreate virtually all of the movements of the cell phone, and hence its user, twenty-four hours a day.

Roberts, writing for the majority, recognized the breadth of the data CSLI could provide the police:

> [H]istorical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike . . . the car in *Jones*, a cell phone—almost a “feature of human anatomy”—tracks nearly exactly the

---

85. See id. at 397 (noting cell phone user can get any information at “tap of . . . screen”).
87. See id. at 397-98 (calling attention to vast scope of accessible information in potential search of cell phone).
88. See id.
90. See id. at 2211-12 (summarizing creation of CSLI).
movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person’s movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in Jones, police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the government’s view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.91

The greater the concentration of cell sites, such as in urban areas, the smaller the coverage area of each cell tower and the more precise the tracking of the cell phone.92 Like the phone company in Miller, cell phone service providers maintain this data largely for business purposes, such as in “finding weak spots in their network and applying ‘roaming’ charges when another carrier routes data through their cell sites[, or to] . . . sell aggregated location records to data brokers, without individual identifying information of the sort at issue here.”93 In Carpenter, the government sought to obtain CSLI data with a court order pursuant to a federal statute, the Stored Communications Act,94 which established a bar lower than probable cause to obtain such information from a third-party provider. All the government needed to demonstrate to a magistrate or judge was “specific and articulable facts showing that there are reasonable

91. Id. at 2218 (citations omitted).
92. See id. at 2211-12 (detailing use of cell towers and impact on cell providers).
93. See Carpenter, 138 S. Ct. at 2212.
grounds to believe” that the records sought were “relevant and material to an ongoing criminal investigation.”

In the decision for the majority, Roberts noted the broad purposes of the Fourth Amendment: to secure “the privacies of life” against “arbitrary power,” and “to place obstacles in the way of a too permeating police surveillance.”

He recognized that in a prior case, Kyllo v. United States, the Court had found that the government violated Fourth Amendment rights by pointing a thermal imaging device at a house without a search warrant, and thereby prohibited the government from invading privacy with the then-new technology. He further noted that in Riley, the Court had imposed further limits on the traditional Fourth Amendment search incident to arrest exception to guard against another form of privacy invasion through technology, the modern cell phone. But these cases were decided against the backdrop of the third-party doctrine without addressing it directly. Carpenter presented that direct conflict required the Court to re-examine established law and reconcile “two lines of cases, both of which inform our understanding of the privacy interests at stake”: the third-party doctrine cases of Miller and Smith—because CSLI, like the dialed telephone numbers at issue in Smith, was created and held by third-parties—and the line of cases “addresses[ing] a person’s expectation of privacy in his physical location and movements” compromised through technology, the issue highlighted by Sotomayor in Jones.

In striking the balance, Roberts rejected a simple application of Smith and Miller in these circumstances, finding that the logic of Smith and Miller, which focused on limited historical records maintained by third parties, did not extend to the qualitatively different category of cell-site location data, which did not simply reflect dialed numbers but rather provided “a detailed and comprehensive record of the person’s movements.” Because this was so, the Court:

decline[d] to extend Smith and Miller to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location

96. See id. at 2214 (highlighting Court’s attempt to protect Fourth Amendment privacy rights amidst advanced technology).
98. See id. at 34-36 (noting privacy right remains “entirely unaffected by . . . advance of technology); see also Carpenter, 138 S. Ct at 2214.
99. See Riley v. California, 573 U.S. 373, 393 (2014); see also Carpenter, 138 S. Ct at 2214.
100. See Carpenter, 138 S. Ct at 2214-16 (comparing expectation cases with third-party doctrine cases).
information obtained from Carpenter’s wireless carriers was the product of a search.102

Indeed, Roberts found that “[a] majority of [the] Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements at least for long periods of time,” citing to Sotomayor’s and Alito’s concurrences in Jones.103

Roberts further rejected the idea that because the cell phone companies created the CSLI without the user’s knowledge undermined the users expectation of privacy in it. Again citing Sotomayor, Roberts noted that “[a]s with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”104 The government’s proposed straightforward application of the third-party doctrine under Miller and Smith to these circumstances ignored the drastic changes in technology “that made possible the tracking of not only Carpenter’s location but also everyone else’s . . . for years and years. . . . There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today.”105 The government, the Court found, was thus “not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.”106

Further, unlike in Smith and Miller, there was no voluntary exposure by the cell phone user of CSLI information in Carpenter; instead, the cell companies instead automatically captured that information.107 “As a result, in no meaningful sense does the user voluntarily ‘assume[] the risk’ of turning over a comprehensive dossier of his physical movements,”108 as was the case in Smith and Miller. Nevertheless, despite the criticism of the third-party doctrine, Roberts wrote that the Carpenter decision was narrow and did not “disturb the application of Smith and Miller.”109

Thus, even though the cell phone user’s CSLI data was in the hands of a third party in Carpenter, that fact did not provide the government with the authority to obtain it without a warrant. The fact that it was the government that was seeking the data made a difference in the analysis. Coupled with Jones and Riley, this suggests that when it is the government that is the party seeking access, the

102. Id.
103. See id. (offering support for Court’s decision founded in society’s general privacy expectation).
104. See id. (citations omitted).
105. See Carpenter, 138 S. Ct. at 2219.
106. Id.
108. See id. (citation omitted).
109. See id. at 2220.
Court will put up a barrier to access where one did not exist against other third parties.

V. ANALYSIS

Jones, Riley, and Carpenter expanded the scope of privacy rights protected under the Fourth Amendment, even if their logic conflicts at some level with Smith and Miller. Carpenter left Smith and Miller as good law, but rejected their assumption of risk idea—at least as to CSLI, information created not at a user’s request but for the convenience of a data-provider. This makes sense; the notion that cell phone users are choosing to waive their privacy by participating in a digital world is a troubling one. Is there any real choice but to have a cell phone? Or to keep personal records digitally, the equivalent of the locked cabinet from days gone by? Can one really participate in society without text and email? Or without social media, when much of the political discourse in America takes place through that medium? At least in many cases, we are not thereby choosing to waive privacy rights simply by engaging in digital discourse, or assuming a risk by doing so.

With Smith and Miller still good law, the expectation of privacy analysis from Katz is problematic in the digital world, since almost everything on a cell phone is shared with a third party. In his dissent in Carpenter, Justice Gorsuch makes that very point.110 But even if an expectation of privacy survives despite the access a third party may have, that expectation is nonetheless vulnerable on its merits. An expectation of privacy is only viable if it is reasonable. It is one thing if a cell phone service provider created a species of data, like CSLI, without a user knowing about it and, and the Court found some form of privacy waiver by the user over that data simply by using the cell phone. That does not seem like an assumption of the risk at all, where the risk is entirely unknown to the user. But once the existence of data like CSLI becomes widely known, what then? What becomes of that expectation of privacy if we become increasingly aware that the third parties to whom we have entrusted our presumably private information have access to, and may even exploit, such information? Then is it fair to consider use of a cell phone an assumption of the risk? The press has reported that Facebook allowed data mining of its users’ data during the 2016 presidential election.111 It appears Google has access to the substance of messages sent using Gmail.112 What if other companies exploit what we think is

110. Id. at 2261-62 (Gorsuch, J., dissenting).
private data for their own benefit, and that fact becomes common knowledge? Is it the case that the expectation of privacy becomes unreasonable, and we assume a risk even if we cannot avoid doing so?

If the assumption of risk idea is to continue, it may well be that those user agreements most users of technology reflexively accept—for cell phone service, for email service, or for services like Facebook, SnapChat, and Instagram—may become far more meaningful. What those agreements say about waivers of privacy rights might matter if the issue becomes the reasonableness of an expectation of privacy. Note that the Court in Smith refused to permit the billing practices of the telephone company dictate the scope of privacy, and that neither Riley nor Carpenter examined the user agreements the companies providing the services had with the cell phone user. But it is not hard to imagine that the government may seek to make use of these agreements in arguing that expectations of privacy are unreasonable if those contracts include broad waivers of privacy rights.

More troublingly, there is a risk that privacy rights will be diluted if invasion of them becomes the norm—not the unique practice of a given company, but the widespread and tolerated practice of an entire industry. Based on a straightforward Katz analysis, there may be no reasonable expectation of privacy under those facts. Indeed, in Kyllo, the Court observed that “[w]e think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ constitutes a search—at least where (as here) the technology in question is not in general public use.”\(^\text{113}\) That language suggests the obvious—that if a violation of privacy rights becomes routine, the expectation of privacy ends.

But even if the Court expands privacy protection to include data held on behalf of citizens by third parties, the law still must address the greater notion of openness in the digital world, the promotion of sharing of information far and wide. In many cases, users voluntarily share such data with others. When they do so, the question arises as to how much privacy a user can expect, and whether a user can argue that sharing with non-police should not be considered a waiver of privacy as to the police.

Take a modern app like SnapChat. SnapChat facilitates the sharing of photos, videos, and the like. Like other apps, it provides a user with the ability to restrict access of others to his or her account to only those the users recognizes as “friends.” Assume an undercover agent poses as a “friend” and gains permission from the user to access the account. Would it matter that the user did not know that it was the police who sought access? Federal law has long permitted the government to pose as criminal confederates and obtain consent to receive

otherwise private, criminal communications. In contrast, some federal courts have found that the government generally cannot obtain valid consent to access private locations where that consent is based on the government agent’s posing as a law-abiding private citizen. For instance, if the police gain access to a house while posing as a gas company employee searching for a gas leak, the consent may be unlawful. What if the police do neither, but rather just ask for access using a false name and get it? Is it the case that the user has then truly accepted the risk—that by accepting a request from a person who was unknown to him or her, doing so undercuts any argument that the user relied on privacy safeguards provided by Snapchat to protect the privacy of Snapchat posts? Some lower federal courts think so. Is that what the law should be?

Carpenter suggests that if it is the government that is doing the asking, the standard for finding of Fourth Amendment waiver might be different that if another citizen was doing the asking. If that is so, it would allow users to share data with citizens but still expect privacy vis-a-vis the police, a potentially significant protection. But how far would that protection go?

Take an extreme version of data sharing that raises the question of just when a citizen waives his or her privacy rights, or at least assumes the risk of disclosure in such a manner that the data may no longer be private and within the scope of Fourth Amendment protection. What if a citizen takes extremely personal, telling data and voluntarily provides it to a third party expressly to analyze it and share the results with others? Would that information be private under current Fourth Amendment law? DNA analysis is now provided by a number of companies, including Ancestry.com and 23andMe. DNA analysis provides the most private details of our physical lives, like parentage or susceptibility to disease. DNA is also an information bonanza for law enforcement, as it allows the police to match DNA found at crime scenes to suspects, often with astonishing accuracy. Despite the potential for use of this information by law enforcement, citizens willingly provide their DNA—and by extension, that of their family members—to third-party companies.

In some cases, users elect to share the data with others for their own purposes, such as to find other family members. But even if they do not, the data still

---


116. Cf., e.g., Everett v. State, 186 A.3d 1224, 1236 (Del. 2018); United States v. Gatson, No. 13–705, 2014 WL 7182275, at *22 (D.N.J. 2014) (finding no warrant required for officer using undercover account to become Instagram “friends” with defendant); United States v. Meregildo, 883 F. Supp. 2d 523, 525-26 (S.D.N.Y. 2012) (holding Facebook user’s act of sharing post terminates privacy expectation). The court in Everett specifically stated “the Fourth Amendment does not guard against the risk that the person from whom one accepts a ‘friend request’ and to whom one voluntarily disclosed such information might turn out to be an undercover officer or a ‘false friend.’” Everett, 186 A.3d at 1236.
exists, and the government can access it; the only remaining issue is whether they do so with or without a search warrant. In California, police identified a man they believe to be the Golden State Killer, a serial killer allegedly responsible for at least a dozen murders and dozens of rapes in the 1970s and 1980s, through DNA without the use of a warrant or even a court order. They posted a sample of the suspect’s DNA profile on GEDmatch, which is a free open-source website that pools together genetic profiles uploaded by users seeking to conduct research on, or fill in gaps in, their family trees. The results led law enforcement to the suspected killer’s distant relatives, who evidently were among the millions of consumers who voluntarily posted their DNA profile on the site.

Even where a user seeks to protect his or her privacy, the reality is that users are voluntarily creating data of tremendous value to law enforcement that did not exist in the past. The reality that the Court addressed in Jones, Riley, and Carpenter is that highly-revealing data sought by the police existed—data that would not have realistically have been available to the police in the past. Even if it is protected under Fourth Amendment privacy concepts, the police, with very rare exceptions likely inapplicable to digital searches, still can access it with search warrants. So even if the Court extends privacy protection to data held by third parties, the police can still obtain that information with a search warrant and will enjoy the benefit of information that would otherwise not have been obtainable in the past.

Thus, as technology expands, the risk to privacy follows. The law accords cars less privacy than homes. As cars increasingly become equipped with monitoring systems—internal ones built into them by manufacturers, or external ones, like “EZ Pass” transponders, added to them by owners—these systems create data that permit third parties to track information about the location and use of the vehicles. As the majority in Jones pointed out, one’s movements on public roads is not typically protected by the Fourth Amendment. So can


118. See id.

119. See id.

120. See Winston v. Lee, 470 U.S. 753, 759 (1985). “A compelled surgical intrusion into an individual’s body for evidence, however, implicates expectations of privacy and security of such magnitude that the intrusion may be ‘unreasonable’ even if likely to produce evidence of a crime.” Id. In rare cases, an intrusion into the human body may be justified by probable cause but still be unreasonable, and therefore unlawful, under the Fourth Amendment. Id.


police, who commit no trespass, access EZ Pass data without a warrant and not run afoul of Carpenter? Even if Carpenter protects that data, all the government needs to is get a warrant to obtain detailed information about a user’s movements—information that a user may have involuntarily or voluntarily permitted to be created. Home devices now “listen” to communication in the home; some, like Amazon’s Alexa or Google’s Assistant, do only that. Police who are lawfully in a home could not simply query such devices if they happen to be in a home under plain view principles. But there would be no restriction to their getting warrants and doing just that. Personal fitness devices, like “Fit Bits,” track deeply personal, physical information about a user. The same dangers arise with these: Once the data exists, the government may find a way to obtain it.

The point is that users assume risks in using these devices and services and creating this data. Under at least some circumstances, the government may have a strong argument to obtain the information without a search warrant on some basis, such as where the data sought is not overly revelatory, where no trespass was committed in accessing it, or perhaps where the user assumed the risk of exposing the data to others. But in the worst case, the data exists, in some instances because the user permitted it to exist, and once it exists, the government has every incentive to seek to assemble a search warrant to get it. If it does so, privacy is degraded just a bit more, regardless of what Fourth Amendment barriers are erected to restrict access to it. It may be, then, that permitting the data to exist at all is the real risk users assume.

VI. CONCLUSION

The digital age has suddenly presented tools that provide a wealth of opportunities to connect with one another. Law enforcement will seek to exploit that new openness. Carpenter suggests that the Court will not mechanically apply Fourth Amendment law going forward, and a re-examination of Katz, Miller, and Smith is underway; we should prepare to rethink what privacy means in 2019. The third-party doctrine has issues, anyway—after all, since 1877, the privacy of mail has been recognized even though mail is entrusted to a third person, the postal service. Perhaps the answer will be to re-formulate the expectation of privacy analysis to focus not on whether a person has an expectation of privacy against disclosure to everyone, but whether a person has

We accordingly [have] held . . . that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” Thus, . . . our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

Id.

an expectation of privacy against disclosure to the police. If that were the focus of
the test, citizens could disclose personal information to third-party providers and
other citizens, without losing all claims to privacy against the government in
criminal cases. And perhaps under this analysis, parts of the Stored
Communications Act may be found to be unconstitutional. In all events, that
debate seems to be on the horizon.