Edited for
DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW
to be inserted at p. 331 after United States v. Jones

and

DANIEL J. SOLOVE & PAUL M. SCHWARTZ,
PRIVACY, LAW ENFORCEMENT, AND NATIONAL SECURITY
to be inserted at p. 79 after United States v. Jones
https://www.informationprivacylaw.com/

CARPENTER V. UNITED STATES

138 S. Ct. 2206 (2018)

ROBERTS, C.J. This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements. . . .

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T-Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call

records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose "cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls" during the four-month period when the string of robberies occurred. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion.

At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the . . . robbery was at the exact time of the robbery." Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.

The Court of Appeals for the Sixth Circuit affirmed. 819 F. 3d 880 (2016). The court held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection. *Id.*, at 888 (quoting *Smith v. Maryland*, 442 U.S. 735, 741)). . . .

The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-

site records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

We decline 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 information obtained from Carpenter's wireless carriers was the product of a search.

A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S., at 351-352. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones*, 656 U.S. at 430 (Alito, J., concurring in judgment); *id.*, at 415 (Sotomayor, J., concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.* at 429 (opinion of Alito, J.). For that reason, "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." *Id.* at 430.

Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As 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." *Id.* at 415. These location records "hold for many Americans the 'privacies of life.'" *Riley*, 134 S. Ct. 2473 (quoting *Boyd*, 116 U.S., at 630). And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a "feature of human anatomy"—tracks nearly exactly the 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 polices 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.

The Government and Justice Kennedy contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did "not on their own suffice to place [Carpenter] at the crime scene"; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. Yet the Court has already rejected the proposition that "inference insulates a search." *Kyllo*, 533 U.S., at 36. From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.

At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S., at 36. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

The Government's primary contention to the contrary is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are "business records" created and maintained by the wireless carriers. The Government (along with Justice Kennedy) recognizes that this case features new technology, but asserts that the legal question nonetheless turns on a garden-variety request for information from a third-party witness.

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. 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. The

Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 134 S. Ct. 2473. *Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U.S., at 442. *Smith* pointed out the limited capabilities of a pen register; as explained in *Riley*, telephone call logs reveal little in the way of "identifying information." *Smith*, 442 U.S., at 742. *Miller* likewise noted that checks were "not confidential communications but negotiable instruments to be used in commercial transactions." In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI. . . .

Justice Gorsuch wonders why "someone's location when using a phone" is sensitive, and Justice Kennedy assumes that a person's discrete movements "are not particularly private." Yet this case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.

Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley*. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. *Smith*, 442 U.S., at 745.

We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment. . . .

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs

or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944).

Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records. Although the "ultimate measure of the constitutionality of a governmental search is 'reasonableness,'" our cases establish that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 652-653. Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 134 S. Ct. 2473. . . .

Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant. . . .

Justice Alito overlooks the critical issue. At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers. When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents. See *Riley*, 134 S. Ct. 2473 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents]."). . . .

Fourth Amendment[I]f law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency. . . .

We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

The judgment of the Court of Appeals is reversed, and the case is remanded for further proceedings consistent with this opinion. . . .

KENNEDY, J. dissenting. . . . The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. *United States v. Miller*. This is true even when the records contain personal and sensitive information. So when the Government uses a subpoena to obtain, for example, bank records, telephone records, and credit card statements from the businesses that create and keep these records, the Government does not engage in a search of the business's customers within the meaning of the Fourth Amendment. . . .

Cell-site records . . . are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

The Court today disagrees. It holds for the first time that by using compulsory process to obtain records of a business entity, the Government has not just engaged in an impermissible action, but has conducted a search of the business's customer. The Court further concludes that the search in this case was unreasonable and the Government needed to get a warrant to obtain more than six days of cell-site records.

In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases. In doing so it draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. According to today's majority opinion, the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations. . . .

The principle established in *Miller* and *Smith* is correct for two reasons, the first relating to a defendant's attenuated interest in property owned by another, and the second relating to the safeguards inherent in the use of compulsory process.

First, *Miller* and *Smith* placed necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a "requisite connection." . . . . Fourth Amendment

Miller and *Smith* set forth an important and necessary limitation on the *Katz* framework. They rest upon the commonsense principle that the absence of property law analogues can be dispositive of privacy expectations. The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes. The businesses were not bailees or custodians of the records, with a duty to hold the records for the defendants' use. The defendants could make no argument that the records were their own papers or effects. The records were the business entities' records, plain and simple. The defendants had no reason to believe the records were owned or controlled by them and so could not assert a reasonable expectation of privacy in the records.

The second principle supporting *Miller* and *Smith* is the longstanding rule that the Government may use compulsory process to compel persons to disclose documents and other evidence within their possession and control. . . .

For those reasons this Court has held that a subpoena for records, although a "constructive" search subject to Fourth Amendment constraints, need not comply with the procedures applicable to warrants—even when challenged by the person to whom the records belong. Rather, a subpoena complies with the Fourth Amendment's reasonableness requirement so long as it is "'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be

unreasonably burdensome.'" *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415. Persons with no meaningful interests in the records sought by a subpoena, like the defendants in *Miller* and *Smith*, have no rights to object to the records' disclosure—much less to assert that the Government must obtain a warrant to compel disclosure of the records.

Based on *Miller* and *Smith* and the principles underlying those cases, it is well established that subpoenas may be used to obtain a wide variety of records held by businesses, even when the records contain private information. . . . .

. . . . All this is not to say that *Miller* and *Smith* are without limits. *Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own "papers" or "effects," even when those papers or effects are held by a third party. See *Ex parte Jackson*, 96 U.S. 727, 733 (letters held by mail carrier); *United States v. Warshak*, 631 F. 3d 266, 283-288 (6th Cir. 2010) (e-mails held by Internet service provider). As already discussed, however, this case does not involve property or a bailment of that sort. Here the Government's acquisition of cell-site records falls within the heartland of *Miller* and *Smith*. . . .

THOMAS, J. dissenting. This case should not turn on "whether" a search occurred. It should turn, instead, on *whose* property was searched. The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches of "*their* persons, houses, papers, and effects." (Emphasis added.) In other words, "*each* person has the right to be secure against unreasonable searches . . . in *his own* person, house, papers, and effects." *Minnesota v. Carter*, 525 U.S. 83, 92 (1998) (Scalia, J., concurring). By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint. . . .

The more fundamental problem with the Court's opinion, however, is its use of the "reasonable expectation of privacy" test, which was first articulated by Justice Harlan in *Katz v. United States*, 389 U.S. 347, 360-361 (1967) (concurring opinion). The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence. I respectfully dissent. . . .

At the founding, "search" did not mean a violation of someone's reasonable expectation of privacy. The word was probably not a term of art, as it does not appear in legal dictionaries from the era. And its ordinary meaning was the same as it is today: "'[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo v. United States*, 533 U.S. 27, 32, n. 1. The word "search" was not associated with "reasonable expectation of privacy" until Justice Harlan coined that phrase in 1967. The phrase "expectation(s) of privacy" does not appear in the pre-*Katz* federal or state case reporters, the papers of prominent Founders, early congressional documents and debates, collections of early American English texts, or early American newspapers.

The *Katz* test strays even further from the text by focusing on the concept of "privacy." The word "privacy" does not appear in the Fourth Amendment (or anywhere else in the Constitution for that matter). Instead, the Fourth Amendment references "[t]he right of the people to be secure." It then qualifies that right by

limiting it to "persons" and three specific types of property: "houses, papers, and effects." By connecting the right to be secure to these four specific objects, "[t]he text of the Fourth Amendment reflects its close connection to property." *Jones*, supra, at 405. "[P]rivacy," by contrast, "was not part of the political vocabulary of the [founding]. Instead, liberty and privacy rights were understood largely in terms of property rights." Cloud, Property Is Privacy: Locke and Brandeis in the Twenty-First Century, 55 Am. Crim. L. Rev. 37, 42 (2018).

Those who ratified the Fourth Amendment were quite familiar with the notion of security in property. Security in property was a prominent concept in English law. . . .

ALITO, J. , with whom THOMAS, J. joins, dissenting. I share the Court's concern about the effect of new technology on personal privacy, but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.

First, the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today's decision does, is revolutionary. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent. Unless it is somehow restricted to the particular situation in the present case, the Court's move will cause upheaval. Must every grand jury subpoena *duces tecum* be supported by probable cause? If so, investigations of terrorism, political corruption, white-collar crime, and many other offenses will be stymied. And what about subpoenas and other document-production orders issued by administrative agencies?

Second, the Court allows a defendant to object to the search of a third party's property. This also is revolutionary. The Fourth Amendment protects "[t]he right of the people to be secure in *their* persons, houses, papers, and effects" (emphasis added), not the persons, houses, papers, and effects of others. Until today, we have been careful to heed this fundamental feature of the Amendment's text. This was true when the Fourth Amendment was tied to property law, and it remained true after *Katz v. United States*, 389 U.S. 347 (1967), broadened the Amendment's reach.

By departing dramatically from these fundamental principles, the Court destabilizes long-established Fourth Amendment doctrine. We will be making repairs—or picking up the pieces—for a long time to come. . . .

GORSUCH, J. dissenting. In the late 1960s this Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an "expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (Harlan, J., concurring). Then, in a pair of decisions in the 1970s applying the *Katz* test, the Court held that a "reasonable expectation of privacy" *doesn't* attach to information shared with "third parties." See *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). By these steps, the Court came to

conclude, the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and maybe even your doctor.

What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

What to do? It seems to me we could respond in at least three ways. The first is to ignore the problem, maintain *Smith* and *Miller*, and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set *Smith* and *Miller* aside and try again using the *Katz* "reasonable expectation of privacy" jurisprudence that produced them. The third is to look for answers elsewhere. . . .

Start with the first option . . . Those cases announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it. And even if *Smith* and *Miller* did permit courts to conduct a balancing contest of the kind the Court now suggests, it's still hard to see how that would help the petitioner in this case. Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say. . . .

What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification. The Court has said that by conveying information to a third party you "'assum[e] the risk'" it will be revealed to the police and therefore lack a reasonable expectation of privacy in it. *Smith*. But assumption of risk doctrine developed in tort law. It generally applies when "by contract or otherwise [one] expressly agrees to accept a risk of harm" or impliedly does so by "manifest[ing] his willingness to accept" that risk and thereby "take[s] his chances as to harm which may result from it." Restatement (Second) of Torts §§496B, 496C(1), and Comment b (1965). . . . Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to "manifest my willingness to accept" the risk that the government will pry the document from my friend and read it *without* his consent?

One possible answer concerns knowledge. I know that my friend *might* break his promise, or that the government *might* have some reason to search the papers in his possession. But knowing about a risk doesn't mean you assume responsibility for it. Whenever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he may do to you. . . .

In the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants.. . . .

There's a second option. What if we dropped *Smith* and *Miller*'s third party doctrine and retreated to the root *Katz* question whether there is a "reasonable

expectation of privacy" in data held by third parties? Rather than solve the problem with the third party doctrine, I worry this option only risks returning us to its source: After all, it was *Katz* that produced *Smith* and *Miller* in the first place.

Katz's problems start with the text and original understanding of the Fourth Amendment, as Justice Thomas thoughtfully explains today. *The Amendment*'s protections do not depend on the breach of some abstract "expectation of privacy" whose contours are left to the judicial imagination. Much more concretely, it protects your "person," and your "houses, papers, and effects." Nor does your right to bring a Fourth Amendment claim depend on whether a judge happens to agree that your subjective expectation to privacy is a "reasonable" one. Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period. . . .

Maybe, then, the *Katz* test should be conceived as a normative question. But if that's the case, why (again) do judges, rather than legislators, get to determine whether society *should be* prepared to recognize an expectation of privacy as legitimate? Deciding what privacy interests *should be* recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime. Answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts. We also risk undermining public confidence in the courts themselves. . . .

My concerns about *Katz* come with a caveat. *Sometimes*, I accept, judges may be able to discern and describe existing societal norms. So there may be *some* occasions where *Katz* is capable of principled application—though it may simply wind up approximating the more traditional option I will discuss in a moment. Sometimes it may also be possible to apply *Katz* by analogizing from precedent when the line between an existing case and a new fact pattern is short and direct. But so far this Court has declined to tie itself to any significant restraints like these. As a result, *Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence. *Smith* and *Miller* are only two examples; there are many others. . . .

There is another way. From the founding until the 1960s, the right to assert a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the "reasonableness" of your expectations or privacy. It was tied to the law. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." True to those words and their original understanding, the traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment. . . .

I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right. Where houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title. Both the text of the Amendment and the common law rule support that conclusion. . . .

Another point seems equally true: just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it. Not infrequently one person comes into possession of someone else's property without the owner's consent. Think of the finder of lost goods or the policeman who impounds a car.

[P]ositive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things. In the context of the *Takings Clause* we often ask whether those state-created rights are sufficient to make something someone's property for constitutional purposes.

. . . [W]hile positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it. *Ex parte Jackson* reflects that understanding. There this Court said that "[n]o law of Congress" could authorize letter carriers "to invade the secrecy of letters." So the post office couldn't impose a regulation dictating that those mailing letters surrender all legal interests in them once they're deposited in a mailbox. If that is right, *Jackson* suggests the existence of a constitutional floor below which Fourth Amendment rights may not descend. Legislatures cannot pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause.

[T]his constitutional floor may, in some instances, bar efforts to circumvent the Fourth Amendment's protection through the use of subpoenas. No one thinks the government can evade *Jackson*'s prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster for "all letters sent by John Smith" or, worse, "all letters sent by John Smith concerning a particular transaction." So the question courts will confront will be this: What other kinds of records are sufficiently similar to letters in the mail that the same rule should apply?

NOTES & QUESTIONS

1. ***The Future of the Third Party Doctrine.*** After *Carpenter*, in what situations will the third party doctrine apply? In what situations will it not apply? What test does the Court use to make this determination? Is there a workable test?
2. ***Historical CSLI as Unique?*** The majority opinion rests on a conviction that historic CSLI represents a "seismic shift[] in digital technology" and presents "novel circumstances." It also points to "the unique nature of cell phone location information." Are you convinced that historic CSLI is that different from other kinds of third-party collections of personal data? Moreover, how would one distinguish the historical, long-term records at stake in Carpenter and a one-time "ping" by law enforcement of locational information from a cell phone?
3. ***Justice Alito***. Is Justice Alito's dissent in *Carpenter* consistent with his concurrence in *Jones*? Why does he decide these cases differently?
4. ***A Turn to Property?*** In dissent in *Carpenter*, Justice Gorsuch wishes the Supreme Court to resolve the third party issue under the Fourth Amendment by developing a property-based sense of privacy. In your view, is this area of law potentially more helpful than the established search under *Katz* for reasonable expectations of privacy?