

## Handbook of Environmental Engineering

On Friday, June 22, the Supreme Court issued its much-anticipated opinion in *Carpenter v. United States*, holding that a warrant is required for police to access cell site location information from a cell phone company—the detailed geolocation information generated by a cellphone’s communication with cell towers. As predicted, Chief Justice Roberts authored the majority opinion, reversing the Sixth Circuit’s decision. He was joined by Justices Ginsburg, Breyer, Sotomayor and Kagan. The remaining four justices, Justices Kennedy, Thomas, Alito, and Gorsuch each filed separate dissenting opinions.

### Background

#### Legal Background

The Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA), creates privacy protections for the content of stored communications and the related non-content information. Orders made under Section 2703(d), known as 2703(d) orders, can compel the production of the content of stored communications or related non-content information, when “specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” This standard of suspicion is considerably lower than the probable cause required for a typical warrant.

Also relevant to this decision are three earlier Supreme Court decisions: *United States v. Miller*, which addressed police access to business records held by third parties; *Smith v. Maryland*, which addressed police access to non-content phone records; and *United States v. Jones*, which dealt with police use of a geolocation device.

In *United States v. Miller*, the Court held that a defendant had no right to privacy in his banking records, as they were business records belonging to the bank. In *Smith v. Maryland*, the Court held that police did not require a warrant to use a pen register to monitor a suspect’s outgoing call data. *United States v. Miller* and *Smith v. Maryland* are examples of the application of the third-party doctrine—the legal principle that when an individual voluntarily gives information to a third party, the privacy interest in that information is forfeit. Because *Carpenter* involved records acquired from cell phone companies, the third-party doctrine was critical to the government’s arguments.

In *United States v. Jones*, the court addressed whether police use of a GPS tracking device required a warrant. Although Justice Scalia’s majority opinion focused on the police placement of the device as a trespass, Justices Alito and Sotomayor each focused their concurrence on the idea that monitoring an individual’s location over time is an invasion of privacy on its own. The idea that the aggregation of data over time can create a much more detailed and privacy-invasive picture is referred to as “mosaic theory.” These concurrences were cited frequently in the decision, and, as Orin Kerr described, played a key role in *Carpenter*’s brief.

## Technical Background

At issue in this case was whether cell-site location information (CSLI), could be accessed by law enforcement without a warrant. CSLI is generated when a phone communicates with a cell tower. Sometimes this data is generated by a user's intentional actions"by placing a phone call, sending a text message, or turning the phone on, the user causes the phone to communicate with the nearest cell tower. CSLI can also be generated automatically"when a phone receives a text message, or when the phone sends a periodic update to the network, for example. The greater the concentration of cell towers, the more accurate the location data will be. This means that it is easier to pin down an individual's precise location in an urban area than in a rural one. Cell phone companies keep records of CSLI for business purposes, but this information can be used to reconstruct the movements of a particular phone over a long period of time.

## Factual Background

In April 2011, four men were arrested in connection with a string of armed robberies of Radio Shack and T-Mobile stores. One of these men confessed that the group was responsible for the robberies, and that as many as 15 other men had participated in the crimes as getaway drivers and lookouts. He gave the FBI his personal cell phone number and the phone numbers of the others involved. The FBI then used the man's call logs to identify additional phone numbers he had contacted around the time of the robberies.

The FBI then applied for 2703(d) orders to produce the "transactional records" from 16 phone numbers, including Carpenter's. The transactional records requested included subscriber information, toll records, call detail records, and numbers dialed, as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls." Three magistrate judges found that the FBI had met the standards of suspicion required by the SCA, and issued the requested 2703(d) orders.

## Procedural History

Two of the conspirators, Timothy Carpenter and Timothy Sanders, were eventually charged with aiding and abetting robbery affecting interstate commerce and the use or carriage of a firearm in violation of the Hobbs Act. At trial, the FBI explained that the CSLI acquired through 2703(d) orders had placed the two men's phone within a half-mile to

two miles of each robbery. Carpenter and Sanders sought to suppress the CSLI evidence under the Fourth Amendment, but the district court denied the motion. Both men were convicted, and both appealed.

On appeal to the Sixth Circuit, Carpenter challenged the district court's denial of his motion to suppress the CSLI. Carpenter argued that the acquisition of CSLI through a 2703(d) order was unconstitutional, because it was a search within the meaning of the Fourth Amendment, and should have only been accessible with a warrant based on probable cause. The Sixth Circuit rejected Carpenter's arguments, relying on *Smith v. Maryland* to hold that the data were business records, not protected by the Fourth Amendment.

On June 5, 2017, the Supreme Court granted certiorari. A wide range of amici filed briefs in this case, from Orin Kerr, who wrote in support of the government, to several privacy advocacy organizations who wrote in support of Carpenter. Oral arguments were held on Nov. 29, 2017.

#### Majority Opinion

Chief Justice Roberts's majority opinion begins with a quick lesson on the history of the Fourth Amendment. Quoting the Supreme Court's ruling in *Camara v. Municipal Court of City and County of San Francisco*, he notes that the court has recognized that the amendment's purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." He describes the evolution of Fourth Amendment doctrine from its early days of relating closely to common-law trespass to the development of the "reasonable expectation of privacy" doctrine under *Katz v. United States*, which established the modern understanding that the Fourth Amendment "protects people, not places."

Roberts also notes that the development of technology has required the court to find ways to preserve privacy from the government even when surveillance tools have enhanced the government's ability to "encroach on areas normally guarded from inquisitive eyes." He cites to both *Kyllo v. United States* (which held that a warrant was required for the government to use a thermal imaging device on a home) and *Riley v. California* (which held that a warrant was generally required to search the contents of a cell phone) to illustrate the ways in which changes in technology have necessitated an approach more nuanced than a "mechanical interpretation" of the Fourth Amendment.

Addressing the facts of this case, Chief Justice Roberts writes that CSLI does not "fit neatly under existing

precedents, and that it instead lies at the intersection of two lines of cases—the first line addressing geolocation, and the second addressing the third-party doctrine.

He begins with a discussion of the geolocation cases. He distinguishes *United States v. Knotts*, in which the court held that a warrant was not required to follow a simple beeper placed in a suspect's car, from *Jones*, in which the court held that a warrant was required for the placement of a GPS device. In *Knotts*, the court found that the device simply augmented the police's ability to track an individual's public movements, while in *Jones*, the police used more sophisticated surveillance to track every movement a person makes in that vehicle. Roberts quotes Justice Alito's *Jones* concurrence, noting that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."

Roberts then discusses the third-party doctrine, addressing both *Miller* (which found that no expectation of privacy exists for bank records) and *Smith* (which found the same for phone company records of outgoing numbers dialed). Roberts highlights the court's reasoning in *Smith*, noting that "when Smith placed a call, he voluntarily conveyed the dialed numbers to the phone company by exposing that information to its equipment in the ordinary course of business."

Roberts then turns to the analysis of the question at hand: whether a warrant is required to access CSLI. He immediately highlights the potential privacy impact of CSLI, noting that "[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled," and distinguishes CSLI from the data in the third-party line of cases. "After all," he points out "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."

Roberts expressly declines to extend the third-party doctrine to CSLI. "Given the unique nature of cell phone location records," he states, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."

Instead, he holds "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."

In a footnote, Roberts notes that that court does not specifically hold on whether fewer days of CSLI could be accessed without a warrant (a weeks' worth of records were accessed in Carpenter). "We need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."

Roberts then explains why there is a reasonable expectation of privacy in CSLI, beginning with the privacy interest in location data. He references the concurrences in Jones once again to support the proposition that it is reasonable for society to expect that law enforcement will not catalogue an individual's every movement. With respect to CSLI, he points out that "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."

CSLI, Roberts states, presents an "even greater privacy concerns than the GPS monitoring of a vehicle we considered in Jones," because a cell phone is almost a "feature of human anatomy" (quoting Riley) and "tracks nearly exactly the movements of its owner." Further, he notes that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable," pointing out that the only real limit on the government's ability to gather information is the length of time the data is retained by wireless carriers "which currently maintain records for up to five years."

Roberts goes on:

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 argued that the CSLI obtained in this particular case was less precise than GPS information. But Roberts notes that CSLI accuracy is "rapidly approaching GPS-level precision," and emphasizes the language in Kyllo that the courts "must take account of more sophisticated systems that are already in use or in development."

Roberts then explains why the third-party doctrine does not extend to this data. He notes that "seismic shifts in

digital technology have made it possible for constant location data to be collected on all cellphone users for years. "There is a world of difference," he writes, "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 bank data in Miller and pen register data in Smith, Roberts explains, had a limited ability to reveal sensitive information. But "there are no comparable limitations on the revealing nature of CSLI." He addresses the concerns of the dissenting justices who were skeptical of the sensitivity of this data, writing that "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."

Roberts also distinguishes Smith and Miller on voluntariness grounds. "Cell phone location information is not truly "shared" as one normally understands the term," he explains. Not only is a cell phone "indispensable to participation in modern society," but 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." Because of this, Roberts concludes that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data," meaning that the user does not voluntarily assume the risk of sharing the data.

Roberts concludes his analysis by explaining that the decision is "a narrow one." He clarifies that the Court is not disturbing "the application of Smith and Miller," or "call[ing] into question conventional surveillance techniques and tools, such as security cameras," or "business records that might incidentally reveal location information."

Finally, Roberts holds that a warrant is required for CSLI, and that "an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records." He addresses concerns raised by Justice Alito in his dissent that a court order is typically sufficient to access records, noting that while this is true when there is a diminished expectation of privacy in the records, it is not true in this case, because "CSLI is an entirely different species of business record." He notes that this is not a far-reaching conclusion, stating that law enforcement "will be able to use subpoenas to acquire records in the overwhelming majority of investigations."

Roberts also notes that existing exceptions to the warrant requirement, such as the existence of exigent circumstances, will still apply to CSLI. “While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation,” he explains “the rule we set forth does not limit their ability to respond to an ongoing emergency.”

Roberts concludes by emphasizing once again “the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection,” writing that “the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.”

#### Dissents

The four dissenting justices each filed separate opinions. Justices Thomas and Alito both Joined Justice Kennedy’s opinion, and Justice Thomas joined Justice Alito’s opinion.

#### Justice Kennedy

Justice Kennedy dissents primarily on third-party doctrine grounds, arguing that CSLI is not fundamentally different from other business records, and that the 2703(d) orders were all law enforcement needed to access them. “Cell-site records,” he writes, “are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process.” He finds the distinction Roberts draws between CSLI and other phone or credit card records to be “illogical.”

Notably, Kennedy’s description of the accuracy of CSLI differs starkly from that of Roberts. Where Roberts focuses on current CSLI as approaching GPS levels of accuracy, Kennedy states that “cell-site records reveal the general location of the cell phone user,” and that they can “reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks.”

Kennedy emphasizes the routine business nature of the records, and their importance to wireless service providers. He notes that providers aggregate and sell this data to third parties, and that the “market for cell phone data is now estimated to be in the billions of dollars.” He also notes the important role CSLI plays in criminal investigations, explaining that this data is “uniquely suited” to the task of linking the criminal gang in this case to the

specific robberies they were suspected to have committed.

Kennedy argues that no search within the meaning of the Fourth Amendment occurred in this case. Because, he argues, the records were controlled by a third party, Carpenter lacked a privacy interest in them, and no search occurred in acquiring the CSLI from the wireless providers. He relies on both Miller and Smith to argue that the property-based conceptions of the Fourth Amendment still applyâ€”that â€œindividuals often have greater expectations of privacy in things and places that belong to them, not to others.â€• In Miller and Smith, Kennedy argues, the defendants â€œcould make no argument that the records were their own papers or effects.â€• The records in Miller and Smith â€œwere the business entitiesâ€™ records, plain and simple,â€• and the defendants in those cases â€œhad 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.â€•

Kennedy then turns to the sufficiency of a compulsory process (a court order requiring a lower standard of suspicion than a warrant). He explains the difference, noting that â€œ[w]hile a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure.â€• When a defendant has no privacy interest in the records, as was the case in Miller and Smith, the defendant has no right to object to its disclosure.

Kennedy then describes a number of situations in which a subpoena has been found to be sufficient, noting â€œit 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.â€• He cites credit card records, vehicle registration records, hotel records, employment records, and utility records as examples.

Kennedy argues that Carpenter is like the defendants in Miller and Smith, noting that he â€œcan â€œassert neither ownership nor possessionâ€• of the records and has no control over them.â€• He dismisses Carpenterâ€™s argument that 47 U.S.C. Â§ 222 grants customers an interest in CSLI as their â€œpersonal papers,â€• noting that the â€œstatuteâ€™s confidentiality protections may be overridden by the interests of the providers or the Government.â€• He continues, â€œ[c]ustomers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even their right to request access to the records is limited.â€•

For these reasons, Kennedy argues, “Carpenter lacks a requisite connection to the cell-site records,” and he therefore “may not claim a reasonable expectation of privacy in them.” Kennedy argues that it would have been reasonable for Carpenter to expect that his wireless provider would “use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.”

Kennedy then proceeds with his analysis of the majority opinion. He addresses the geolocation cases (Knotts and Jones), pointing out that while the court in Knotts suggested that its holding would not apply to “dragnet-type law enforcement practices,” this meant “twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision,” and that in this case, there was a “judicial check,” because a magistrate judge issued the 2703(d) orders. He also rejects the majority’s adoption of the concurring opinions in Jones, noting that in Jones, the Court’s holding was that that a search had occurred because the police “physically occupied private property [of the defendant] for the purpose of obtaining information,” and that there had been no court-approved compulsory process in that case.

Kennedy goes on to criticize the majority’s treatment of Miller and Smith. He writes that in his view, the majority opinion appears to read those cases as establishing a balancing test, weighing “the privacy interests at stake” against “the fact that the information has been disclosed to a third party.” Kennedy rejects this reading, stating that “the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy.”

Even if the balancing test is the way to address the third-party doctrine, Kennedy believes that “the Court errs . . . when it concludes that cell-site records implicate greater privacy interests” and thus deserve greater Fourth Amendment protection “than financial records and telephone records.” He argues that “a person’s movements are not particularly private,” stating that “[t]oday expectations of privacy in one’s location are, if anything, even less reasonable than when the Court decided Knotts.” He once again points to the accuracy of the CSLI in this case, noting that it “could not reveal where Carpenter lives and works, much less his “familial, political, professional, religious, and sexual associations.” He also draws similarities between the intimacy of location information and the intimacy of the data in financial and telephone records, as well as similarities in their retrospective reach, and the need to provide this information to third parties to participate in society.

Finally, Kennedy addresses the majority’s emphasis on the march of technology, writing that “future developments

areno basis upon which to resolve this case.â€• He argues that the Court â€œrisks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society becomes clear.â€• He cites Orin Kerrâ€™s equilibrium adjustment theory, explaining that new technology can make both criminal activity and law enforcement easier, and the balance â€œoften will be difficult to determine during periods of rapid technological change.â€• He notes that Congress has weighed in on this issue through the SCA, and that â€œ[t]he last thing the Court should do is incorporate an arbitrary and outside limit . . . and use it as the foundation for a new constitutional framework.â€•

In criticizing the majorityâ€™s opinion, Kennedy notes that CSLI is an important investigative tool, and that imposing a warrant requirement will â€œthe effectiveness of an important investigative tool for solving serious crimes.â€• He notes that CSLI is well suited to helping law enforcement â€œdevelop probable cause to apprehend some of the Nationâ€™s most dangerous criminals.â€• He also writes that the Court did not explain â€œwhat makes [CSLI] a distinct category of information,â€• and that the â€œthe majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line.â€•

Kennedy also criticizes the majority opinion suggestion that â€œthat less than seven days of location information may not require a warrant,â€• noting that â€œnothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.â€• He also notes that the majority leaves open questions of how the decision will affect â€œthe subpoena practices of federal and state grand juries, legislatures, and other investigative bodies.â€•

Kennedy concludes by arguing that when the majority reached the conclusion that the acquisition of Carpenterâ€™s CSLI was a search, it should have remanded to the Sixth Circuit to â€œto â€œdetermine in the first instance whether the search was reasonable.â€• Finally, he states that â€œthe Courtâ€™s reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congressâ€™ power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendmentâ€™s reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search.â€•

Justice Thomas

Justice Thomas's dissent begins with a clear thesis. "This case should not turn on whether a search occurred," he states. "It should turn, instead, on whose property was searched." In *Carpenter*, he argues, the CSLI records belong to MetroPCS and Sprint. He goes a step further than Kennedy, arguing that the reasonable-expectation-of-privacy test "has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law."

Thomas begins with a history of wiretap jurisprudence and its origins in trespass theory, beginning with *Olmstead*, a 1928 case in which the court held that placing an electronic eavesdropping device was not a search because it was placed without physical entry into the defendant's home. He notes that the court relied on *Olmstead* until the 1960s. First, the court in *Silverman* held that a microphone placed through the wall of a home was a search, without relying on *Olmstead's* assertion that "intangible conversations are not persons, houses, papers, [or] effects." Thomas notes that the *Katz* decision in 1967 "rejected *Olmstead's* remaining holding that eavesdropping is not a search absent a physical intrusion into a constitutionally protected area."

Thomas then critiques the *Katz* holding, and the notion that the question of whether a search occurred turns on whether a reasonable expectation of privacy was violated, not on "the presence or absence of a physical intrusion." Thomas notes that the two-pronged reasonable-expectation-of-privacy test, which looks to society's expectations and the individual's subjective expectations in determining whether a privacy interest exists, was presented for the first time during the *Katz* oral argument by a "recent law-school graduate." He explains that, following *Katz*, the two-pronged test was adopted almost immediately, and over time, the subjective prong has been minimized, leaving reasonable societal expectations (the objective prong) as the dispositive factor in Fourth Amendment jurisprudence.

Thomas argues that the reasonable expectation of privacy test "has no plausible foundation in the text of the Fourth Amendment." He quotes the text of the Fourth Amendment, which describes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches," and argues that "the *Katz* test misconstrues virtually every one of these words." At the founding, Thomas argues, "search" did not "mean a violation of someone's reasonable expectation of privacy." Instead, it held the same plain meaning that it does today "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection."

Further, Thomas notes, the word "privacy" does not appear in the Fourth Amendment. Instead, "the text of the Fourth Amendment reflects its close connection to property." At the founding, Thomas argues, "liberty and

privacy rights were understood largely in terms of property rights. He cites to John Locke's Second Treatise of Civil Government, and the English case *Entick v. Carrington* to support his argument that privacy is security in property. He argues that by "shifting the focus of the Fourth Amendment from property to privacy, the Katz test also reads the words "persons, houses, papers, and effects" out of the text, and argues that this misunderstood the Fourth Amendment's original purpose.

Next, Thomas turns to the issue of ownership, stating that the constitution "specifies that the people have a right to be secure from unreasonable searches of "their" persons, houses, papers, and effects," explaining that it should mean that "individuals do not have Fourth Amendment rights in someone else's property." However, Thomas notes, under the Katz test, the court has found that there can be a privacy interest in someone else's property "like someone else's home.

Thomas then addresses Carpenter's cell-site location information. He argues that Carpenter's claim that the CSLI qualifies as his "papers" within the meaning of the Fourth Amendment is "unpersuasive." Thomas notes that no statutes nor Carpenter's contracts with the wireless providers render the data his property. Thomas rejects Carpenter's argument that the privacy provisions of Section 222 of Title 7 of the U.S. code grant him any privacy interest because the statute does not give him ownership of the records.

Next, Thomas addresses the reasonableness aspect of the Katz test. He writes "reasonableness determines the legality of a search, not "whether a search . . . within the meaning of the Constitution has occurred." Citing *Laura Donahue*, he explains that "the word "unreasonable" in the Fourth Amendment likely meant "against reason" as in "against the reason of the common law." Rather than protecting societal expectations of reasonableness he argues, "by prohibiting "unreasonable" searches and seizures in the Fourth Amendment, the Founders ensured that the newly created Congress could not use legislation to abolish the established common-law rules of search and seizure."

The Founders, Thomas argues, "would be puzzled by the Court's conclusion as well as its reasoning." He writes that to the Founders, "a subpoena for third-party documents was not a "search" to begin with, and the common law did not limit the government's authority to subpoena third parties." They would "be confused by this Court's transformation of their common-law protection of property into a "warrant requirement" and a vague inquiry into "reasonable expectations of privacy."

In his final section, Thomas critiques the Katz test for being “unworkable in practice.” One issue is that “[a]s written, the Katz test turns on society’s actual, current views about the reasonableness of various expectations of privacy, which renders it “easily circumvented.” Thomas cites to Chemerinsky in noting that the government could, in theory, “deny privacy just by letting people know in advance not to expect any.” Thomas also notes that the court has never adequately defined “understandings that are recognized or permitted in society.”

Finally Thomas criticizes the court for treating the Katz test as “a normative question” whether a particular practice should be considered a search under the Fourth Amendment, noting that the court’s precedents “bear the hallmarks of subjective policymaking instead of neutral legal decisionmaking.” Thomas concludes his dissent by describing the Katz test as a “failed experiment” and implores the court to reconsider it.

Justice Alito

Justice Alito begins by noting that while he shares concerns about the “effect of new technology on personal privacy, the majority’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.”

Alito’s dissent focuses on two issues: the distinction between a search and an order requiring the disclosure of documents, and the fact that CSLI is the property of the service provider. “By departing dramatically from these fundamental principles,” Alito writes “the Court destabilizes long-established Fourth Amendment doctrine.”

Alito begins with his analysis of the warrant requirement. “The Court’s holding is based on the premise that the order issued in this case was an actual “search” within the meaning of the Fourth Amendment,” Alito writes, “but that premise is inconsistent with the original meaning of the Fourth Amendment and with more than a century of precedent.”

Justice Alito then outlines a brief history of the subpoena, beginning with writs of subpoena issued under the reign of King Richard II in the late 14th century. He describes a shift in the primary use of the subpoena to compel presence or testimony, to the widespread use of the subpoena duces tecum to compel the production of papers, books, and other forms of physical evidence.”

Alito tracks the use of the subpoena to the United States, pointing out that through the Judiciary act of 1789, the First Congress authorized the courts to “compel the production of papers, books, and other forms of physical evidence, whether from the parties to the case or from third parties.” He notes that subpoenas were used regularly to compel the production of documents in criminal cases in the founding era. He points to the prevalence of grand juries to argue that “the Founders must have been intimately familiar with the tools they used” including the subpoena duces tecum.

The history matters, Alito argues, “not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all.” Because the “compulsory production of documents” is “a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state,” the Fourth Amendment does not apply.

Alito continues discussing the history, noting that the Fourth Amendment “was the founding

generation’s response to the reviled “general warrants” and “writs of assistance.” Because a “subpoena duces tecum permits a subpoenaed individual to conduct the search for the relevant documents himself, without law enforcement officers entering his home or rooting through his papers and effects ... subpoenas avoid the many incidental invasions of privacy that necessarily accompany any actual search.” The Founders, he continues “would thus have understood that holding the compulsory production of documents to the same standard as actual searches and seizures would cripple the work of courts in civil and criminal cases alike.”

Justice Alito then acknowledges that the court has held that subpoenas to produce documents can violate the Fourth and Fifth Amendments, citing to an 1886 decision, *Boyd v. United States*, in which the court found an order “unconstitutional because it compelled the production of property to which the Government did not have superior title.” Alito notes that the reasoning in *Boyd* was “confused from start to finish in a way that ultimately made the decision unworkable.”

Alito tracks the development of the law surrounding subpoenas duces tecum through to *Oklahoma Press Publishing Co. v. Walling*, a 1946 case in which the court found that “the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures,” and that the distinction between

searches and compulsory orders â€œmeant that two different standards had to be applied.â€• For a subpoena, Justice Alito explains, the Oklahoma Press court held that â€œa showing of probable cause was not necessary so long as â€œthe investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry.â€•

Justice Alito then turns to the application of this doctrine to CSLI. Alito agrees with Justice Kennedy that â€œno search or seizure of Carpenter or his property occurred in this case.â€• He states that the 2703(d) order clearly meets the Oklahoma Press standard.

Justice Alito then critiques the majority opinion for â€œimposing requirements thatâ€œuntil this pointâ€œhave governed only actual searches and seizures.â€• To the majority, Alito argues â€œthis case is apparently no different from one in which Government agents raided Carpenterâ€™s home and removed records associated with his cell phone.â€•

Alito continues along this line of reasoning, pointing out that the majority does not â€œexplain why that individual should be entitled to greater Fourth Amendment protection than the party actually being subpoenaed.â€• He argues that this â€œoutcome makes no sense, and the Court does not even attempt to defend it.â€• Holding â€œthat subpoenas must meet the same standard as conventional searches,â€• Alito concludes, â€œwill seriously damage, if not destroy, their utility.â€•

Alito then turns to the second issue he identifies: whether â€œa defendant has the right under the Fourth Amendment to object to the search of a third partyâ€™s property.â€• In an analysis that mirrors Kennedyâ€™s dissent, Alito argues that the CSLI records â€œbelong to Carpenterâ€™s cell service providers, not to Carpenter.â€• Alito explains that because Carpenter had â€œno meaningful control over the cell-site records,â€• and that the Telecommunications Act (47 U.S.C. Â§ 222) provides no basis for a property right in the data, â€œthere is no plausible ground for maintaining that the information at issue here represents Carpenterâ€™s â€œpapersâ€œ or â€œeffects.â€•

Alito then turns to the third-party doctrine, addressing Miller and Smith. He agrees with Kennedy that this line of cases is best understood as placing â€œlimits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a â€œrequisite connection.â€• Because â€œCarpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider,â€• Alito concludes that Carpenter â€œmay not seek to use the Fourth Amendment to exclude them.â€•

Concluding his dissent, Alito speculates on the effect the majority opinion will have on the use of the subpoena. "One possibility" he suggests "is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas duces tecum and all other orders compelling the production of documents will require a demonstration of probable cause." Another is "that this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered."

Finally, he stresses that this issue was already addressed by legislation. The SCA "restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do." He argues that legislation is a better way to address technological change, writing that it "is much preferable to the development of an entirely new body of Fourth Amendment case law for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."

"The desire to make a statement about privacy in the digital age," he writes "does not justify the consequences that today's decision is likely to produce."

Justice Gorsuch

Justice Gorsuch structures his dissent around three possible solutions to the problems of the reasonable expectation of privacy test. First, "ignore the problem, maintain Smith and Miller, and live with the consequences." Second, set Smith and Miller aside and try again using the Katz "reasonable expectation of privacy" jurisprudence that produced them. The third solution, Gorsuch suggests, "is to look for answers elsewhere."

Gorsuch begins with the solution of maintaining Smith and Miller. He agrees with Justice Kennedy's criticism of the majority's proposed balancing test. Smith and Miller "announced a categorical rule," he writes: "Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it." He also questions the majority's finding that location information is more sensitive than numbers dialed or financial records.

Gorsuch then criticizes Smith and Miller, and the third-party doctrine generally. "Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights?" Gorsuch asks. "Can

it secure your DNA from 23andMe without a warrant or probable cause? Smith and Miller say yes it can. He indicates doubt in the premise of the third-party doctrine, noting that if it is "supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be "never" seems a pretty unattractive societal prescription.

Gorsuch then proceeds to analyze the development of the third-party doctrine. He addresses the "assumption of risk" model, which finds its roots in tort law. He argues that the rationale of the tort law model "has little play in this context," and notes that even in tort law, "knowing about a risk doesn't mean you assume responsibility for it." He also discusses consent theories of the third-party doctrine, arguing that "[c]onsenting to give a third party access to private papers that remain my property is not the same thing as consenting to a search of those papers by the government" (emphasis in original). He argues that Smith and Miller ultimately stand for the proposition that Katz "lets the government search almost whatever it wants whenever it wants."

He then turns to the second option "returning to the root Katz question whether there is a "reasonable expectation of privacy" in data held by third parties." This option, Gorsuch concludes, does not solve any problems. Like Thomas, Gorsuch discusses the text of the Fourth Amendment, and notes that its "protections do not depend on the breach of some abstract "expectation of privacy" whose contours are left to the judicial imagination.

Like Thomas, Gorsuch looks to the history of the Fourth Amendment, noting that 18th century cases addressing general warrants and writs of assistance prompted the Founders to address privacy protections. The Founders, Gorsuch notes "chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things" "persons, houses, papers, and effects" and against particular threats "unreasonable" governmental "searches and seizures."

He highlights other problems with the reasonable expectation of privacy test, noting that it is unclear whether it is intended to pose an empirical question or a normative one. Regardless of whether it is an empirical or normative test, Gorsuch questions "why judges rather than legislators should conduct it." He argues that the legislature is better suited to answer these questions noting that "answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts."

Gorsuch does not deny that judges may sometimes "be able to discern and describe existing societal norms," but argues that the Court has yet to tie itself to any particular principled application of Katz. He discusses a few Fourth Amendment cases that produced results he considers "unpredictable" and sometimes "unbelievable" including Florida v. Riley in which the court found no reasonable expectation of privacy from a helicopter flying 400 feet above a person's property, and California v. Greenwood in which the Court found no reasonable expectation of privacy existed in garbage put out for collection.

With respect to data privacy in particular, Gorsuch argues that relying on Katz will lead to continued unpredictable results. He criticizes the majority opinion for not supplying lower courts with significant guidance, noting that it did not address "whether there is any sufficiently limited period of time" for which CSLI can be obtained without a warrant.

Gorsuch also raises questions about the majority silence on real-time CSLI and tower dumps, asking "what distinguishes historical data from real-time data, or seven days of a single person's data from a download of everyone's data over some indefinite period of time?" Gorsuch also criticizes the majority for creating "a second Katz-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the "category of information" so disclosed."

In summing up the first two solutions, Gorsuch notes that they leave lower courts "with two amorphous balancing tests, a series of weighty and in-commensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition."

Gorsuch then turns to the third solution "looking for guidance elsewhere. Unsurprisingly given his line of questioning at oral argument, he finds this guidance in property law. "We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection" he notes. "But what kind of legal interest is sufficient to make something yours?" Gorsuch does not "begin to claim all the answers" but raises a series of questions with which to address the issue.

First, he turns to the concept of bailments to argue that "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them." He quotes the Black's Law Dictionary definition, which defines bailments as "delivery of personal property by one person (the bailor) to

another (the bailee) who holds the property for a certain purpose. He cites to *Ex parte Jackson*, which found a privacy interest in the contents of sealed letters in the mail, to support the proposition that this idea is already reflected in Fourth Amendment jurisprudence. “Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party, Gorsuch argues “may not mean you lose any Fourth Amendment interest in its contents.

“[C]omplete ownership or exclusive control of property, Gorsuch continues, is not always a necessary condition to the assertion of a Fourth Amendment right. He notes that individuals may have a privacy interest in a home they do not own, even when they “merely occupy it for free.

Gorsuch also argues that “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, and analogizes the storage of data with third parties to an involuntary bailment, as in cases of lost goods being found, or the contents of an impounded car.

Next, Gorsuch looks to the Takings Clause, which often requires courts to ask whether those state-created rights in tangible and intangible things “are sufficient to make something someone’s property for constitutional purposes. He suggests that “a similar inquiry may be appropriate for the Fourth Amendment. Pointing to state court opinions and legislation, he notes that “state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.

Gorsuch also argues that although positive law can help to establish a Fourth Amendment interests, “there may be some circumstances where positive law cannot be used to defeat it. He argues that “[l]egislatures cannot pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause.

Finally, Gorsuch notes that the Fourth Amendment’s protections cannot be evaded through the use of subpoenas. “No one thinks the government can evade *Jackson*’s prohibition on opening sealed letters without a warrant, Gorsuch posits “simply by issuing a subpoena to a postmaster for “all letters sent by John Smith.” Courts will need to address “what other kinds of records are sufficiently similar to letters in the mail that the same rule should apply. Gorsuch does not have an answer to this question, indicating that he is “content to adhere to *Jackson* and

its implications for now,â€• although he also warns against restricting the use of subpoenas.

Concluding his dissent, Gorsuch states that he does not â€œagree with the Courtâ€™s decision today to keep Smith and Miller on life support and supplement them with anew and multilayered inquiry that seems to be only Katz-squared.â€• He suggests looking to a â€œmore traditional Fourth Amendment approach,â€• and laments the fact that Carpenter did not pursue a line of argument based on property rights and positive law. â€œI cannot help but concludeâ€œreluctantlyâ€œthat Mr. Carpenter forfeited perhaps his most promising line of argument.â€•

#### Final Notes

Notably, this result should have little effect on Timothy Carpenterâ€™s future. Under the good faith doctrine, established by United States v. Leon, evidence cannot be suppressed at trial when law enforcement relies on a defective court order in good faith. In this case, even though the 2703(d) orders have been deemed insufficient to access CSLI, the police relied on them in good faithâ€œso the suppression remedy is not available to Carpenter. The case has been remanded to the Sixth Circuit, but this decision is unlikely to have any impact on Carpenterâ€™s convictions.

## Reference

[Technical Engineering Notebook Black](#)

[Autodesk Inventor 2023 and Engineering Graphics: An Integrated Approach](#)