Carpenter v. United States 138 S. Ct. 2206 (2018)

CERA J. ARMSTRONG*

BACKGROUND

Cell Site Location Information ("CSLI") is a timestamped record created every time a cell phone connects to a radio-antennae, called a "cell site."[1] Cell sites are comprised of directional antennas that divide service areas into sectors. Usually found on towers, cell sites can also be found on common public fixtures to increase the geographic concentration of cell sites and create stronger cellular networks. Cell phones scan multiple times per minute to connect with cell sites.

Wireless carriers store and collect CSLI for business purposes, including finding weak areas in their networks and applying roaming charges. Though it has been a longtime practice for wireless carriers to retain CSLI from the initiation and termination of incoming calls, recent practice includes collecting information from text transmission and routine data connections, thus creating "vast amounts of increasingly precise CSLI."[2]

After a series of robberies occurred at Radio Shack and T-Mobile stores in the Detroit, Michigan area, a suspect in those robberies identified petitioner Timothy Carpenter ("Carpenter") as an accomplice in a total of nine robberies that occurred in Michigan and Ohio. Carpenter's cell phone number was provided to the FBI. A federal magistrate judge granted two court orders under 18 U.S.C. § 2703(d) of the Stored Communications Act ("D order")[3], allowing the government to compel four months' worth of CSLI from Carpenter's wireless carriers (Metro PCS and Sprint) at initiation and termination of incoming and outgoing calls during the period that the robberies transpired.

The first order granted the government 152 days of CSLI from Metro PCS, which produced 127 days' worth of records.[4] The second order granted the government seven days of CSLI from Sprint, which produced two days of records from when Carpenter's phone was roaming in Ohio.[5] Overall, the government obtained 12,898 data points, averaging 101 points

* Cera J. Armstrong is a 2020 Juris Doctor candidate at the University of San Francisco School of Law.

1. Carpenter v. U.S., 138 S. Ct. 2206, 2211 (2018).
2. *Id.*
3. *Id.* at 2212.
4. *Id.*
5. *Id.*

per day. The data points catalogued Carpenter's intrastate movements and linked Carpenter to the crimes.

PROCEDURAL HISTORY

Carpenter was indicted on six counts of robbery and six counts of carrying a firearm during a federal crime of violence. Before trial, Carpenter filed a motion to suppress the use of CSLI, arguing that the seizure of CSLI violated the Fourth Amendment because it was obtained without a warrant or a warrant exception. The district court denied the motion. At trial, an expert witness for the prosecution used CSLI to produce maps linking Carpenter's phone to the scene of the robberies. Convicted of all but one firearm count, Carpenter was sentenced to more than 100 years in prison.

The Sixth Circuit affirmed the trial court's decision, stating that CSLI was less precise than GPS tracking in U.S. v. Jones.[6] Analogizing the location data of CSLI to the numerical information of phone numbers in Smith v. Maryland,[7] the Sixth Circuit held that CSLI was not protected by the Fourth Amendment and that the government's collection of CSLI did not constitute a warrantless search. Carpenter petitioned for certiorari, which the Supreme Court granted.

ISSUE

The Court addressed whether the collection of historical CSLI data obtained from a wireless carrier constituted a "search" under the Fourth Amendment and thereby necessitated a warrant supported by probable cause.

DECISION

In a decision delivered by Chief Justice Roberts, the Supreme Court held that the government's acquisition of historical CSLI data from a third-party wireless carrier constituted a search under the Fourth Amendment, reversing and remanding the Sixth Circuit's decision.

REASONING

The Court began its analysis distinguishing two threads of Fourth Amendment jurisprudence to determine whether a Fourth Amendment search occurred: (1) the historical property rights approach; and (2) the reasonable expectations of privacy approach. Under the traditional property approach, the Fourth Amendment protects an individual's property rights to their "persons, houses, papers, and effects" from physical trespass.[8] In this case, the Court declined to apply the traditional approach, acknowl-

6. *See generally* U.S. v. Jones, 132 S. Ct. 945 (2012).

7. *See generally* Smith v. Maryland, 99 S. Ct. 2577 (1979).

8. U.S. Const. amend. IV.

edging that when applied to modern technology such as CSLI, analysis under property rights requiring physical trespass does not provide the same level of privacy protections guaranteed under the Fourth Amendment. Instead, the Court applied the reasonable expectations of privacy approach established by Justice Harlan's concurrence in *Katz v. United States*, stating that Fourth Amendment protections extend to individuals in situations where an expectation of privacy is reasonable and one that society is ready to recognize.[9]

Relying on *Katz*, the Court analyzed the government's collection of CSLI from a wireless carrier, holding that, although it lies squarely at the intersection of cases of GPS location data[10] and the third-party doctrine,[11] the collection of CSLI nevertheless constituted a search under the Fourth Amendment.

First, the Court analyzed the collection of historical CSLI using the precedential perspective applied to GPS location data in the *Jones* decision. Relying on the *Katz* reasoning articulated in Justice Alito's and Justice Sotomayor's *Jones* concurrences, the Court held that an individual has a reasonable expectation of privacy to their physical movements captured through CSLI because, like location data collected from GPS tracking, the concentration of cell sites in sectors creates CSLI location data that provides "near perfect surveillance"[12] of an individual's movements. The Court held since almost every individual carries a cell phone that generates CSLI, the privacy interest regarding an individual's movements created by CSLI is one that society is ready to recognize. Overall, the Court held that an individual has a reasonable expectation of privacy to historical CSLI because the accuracy of its location data delivers an intimate window into a person's movements and life, which is a privacy interest that society is ready to recognize.

Second, the Court analyzed whether CSLI, collected and maintained by wireless carriers, qualified as a business record under the third-party doctrine, rendering Carpenter as having a diminished expectation of privacy to the CSLI. Relying on *Smith and Miller*, the Court used both a strict application and the voluntary exposure rationale to show that the third-party doctrine did not extend to CSLI.

The Court first acknowledged that under the strict application, a person's business records have a diminished expectation of privacy that is not protected by the Fourth Amendment. Though historical CSLI stored by wireless carriers is a business record, the Court held that CSLI was distinguishable from the numerical data provided by a pen-register in *Smith* and the checks identified as "negotiable instruments of commercial transactions" in *Miller* because historical CSLI provides a detailed chronicle of an individual's everyday movements. As stated in *Jones*, individuals have a rea-

9. *See generally* Katz v. U.S., 88 S. Ct. 507 (1967).

10. *See generally* U.S. v. Jones, 132 S. Ct. 945 (2012).

11. *See generally* Smith v. Maryland, 99 S. Ct. 2577 (1979).

12. *Carpenter*, 138 S. Ct. at 2218

sonable expectation of privacy in these movements, rendering a strict application of the third-party doctrine inapplicable to CSLI.

The Court then moved to the voluntary exposure rationale, which states that an individual has a diminished expectation of privacy to information they voluntarily expose to a third-party. The Court held that this rationale does not apply to CSLI because an individual's exposure of CSLI to a wireless carrier is not necessarily voluntarily; nearly every individual has to carry a cell phone which automatically generates CSLI without an affirmative action by the user. This means that no cellphone user ever voluntarily assumes the risk of turning their location data over to a third-party. As such, the voluntary exposure rationale does not apply, rendering the third-party doctrine as inapplicable to CSLI.

Finally, the Court concluded its analysis by stating its narrow decision does not include real-time CSLI or "tower dumps;" other business records that accidentally reveal location data; other surveillance techniques and tools; address foreign affairs or national security; and does not overturn *Smith* or *Miller.*[13]

By holding that an individual has a reasonable expectation of privacy to the location data stored and maintained by wireless carriers through historical CSLI, the Court held that the Fourth Amendment protections apply. The Court, in a narrow decision, determined that acquisition of seven days of historical CSLI constitutes a search requiring a warrant showing probable cause and it specified that the exigent circumstances exception still applies. As a result, the Court held that the "D order" standard requiring a showing that evidence be pertinent to an ongoing investigation fell short of the probable cause standard, rendering the government's warrantless acquisition of Carpenter's CSLI as unconstitutional.

DISSENT: JUSTICE KENNEDY

Joined by Justices Alito and Thomas, Justice Kennedy dissented the majority's opinion, arguing that by holding that a search occurred, the majority's opinion unhinges the property-based framework underpinning the Fourth Amendment because CSLI is a business record. Justice Kennedy contends that the majority misinterpreted *Smith* and *Miller* when it held that CSLI creates a record of location data that is distinctive from other business records, reasoning that historical CSLI is not distinctive because it is created and maintained by a third-party wireless carrier. As such, historical CSLI data belonged to the wireless carrier and not to Carpenter, who had no property rights to those records as either "papers" or "effects." Without those property rights, Carpenter lacked a reasonable expectation of privacy to the CSLI. Thus, the government's acquisition of these documents was not a search under the Fourth Amendment. Finally, Justice Kennedy reasons that because a Fourth Amendment search did not occur, the government's use of a court-approved compulsory process, the D order, was ade-

13. *Id.* at 2220.

quate, rendering the government's acquisition of Carpenter's historical CSLI proper.

Justice Kennedy further critiqued the majority's application of the third-party doctrine, stating that an arbitrary six-day cutoff with no clear guidance on what makes historical CSLI a distinct category of business records will have dramatic consequences to both law enforcement and society as a whole.

DISSENT: JUSTICE THOMAS

Justice Thomas's dissent deconstructed the *Katz* test with the text of the Fourth Amendment to show that the *Katz* test should not be used to determine whether Fourth Amendment protections apply. Where the Fourth Amendment protects an individual from "unreasonable searches" over "their persons, houses, papers, and effects,"[14] Justice Thomas argues that the *Katz* test strays from the Founders' intent because it misconstrues the language of the Fourth Amendment by adding the concept of "privacy;" distorting the word "unreasonable;" and misreading the word "their" and the phrase "persons, houses, papers, and effects." After deconstructing the Katz test, Justice Thomas contends that the precise language of the Fourth Amendment narrows the scope of its application to the property approach. Since the Fourth Amendment uses the word "their" before "persons, houses, papers, and effects," Justice Thomas argues that the historical CSLI tracing Carpenter's location is not protected by the Fourth Amendment because it is a business record that belongs to the service providers, in this case Sprint and Metro PCS. It follows that Carpenter did not have a property interest in those records, and therefore was unable to claim Fourth Amendment protections. Justice Thomas concludes his analysis by stating that the *Katz* test is a "failed experiment"[15] that has courts making policy judgment as opposed to judgments of law.

DISSENT: JUSTICE ALITO

In his dissenting opinion, joined by Justice Thomas, Justice Alito argues that the majority erred in its decision by ignoring the distinction between actual and constructive searches. An actual search occurs when law enforcement enters a property to search through a defendant's private papers and effects. Justice Alito reasons that the actual search aligns with the Founders' understandings when drafting the Fourth Amendment protections of a warrant requiring a showing of probable cause. A constructive search occurs when law enforcement compels production of a third-party's documents for evidence pertaining to the defendant. Justice Alito uses the history of the subpoena duces tecum to argue that the Founders intended the use of subpoenas or like processes. Arguing that Fourth Amendment

14. U.S. Const. amend. IV.

15. *Carpenter*, 138 S. Ct. at 2246.

rights cannot be asserted vicariously, Justice Alito reasons that, since historical CSLI belongs to third-party wireless carriers and not Carpenter, historical CSLI does not require Fourth Amendment protections and can be compelled through processes such as a "D order" or subpoena.

DISSENT: JUSTICE GORSUCH

Justice Gorsuch dissented, recognizing that the "reasonable expectations of privacy" test in *Katz* was applied to third-party documents in *Smith* and *Miller*, thereby creating the third-party doctrine which, when applied to this case, allows the government to review any material on a third-party server based on the wrongful theory that "no one reasonably expects any of it will be kept private."[16] Justice Gorsuch proposes three ways to respond: (1) ignore the problem and live with the consequences of *Smith* and *Miller*; [17] (2) set aside *Smith* and *Miller* and use only the *Katz* test;[18] or (3) use the traditional property approach to invoke positive law.

Justice Gorsuch argues that the first proposition is ineffective because the reasoning behind the third-party doctrine in *Smith* and *Miller* is unclear and provides the government with nearly unlimited powers of search. He then argues that the second proposition is also ineffective because *Smith* and *Miller* were decided using the *Katz* test, rendering the unclear justification for the *Katz* test as the root of the issue. As a result, there is further unpredictability in the Fourth Amendment jurisprudence. Finally, Justice Gorsuch argues in favor of the third proposition, reasoning that the limitations of the *Katz* test can be offset by the application of the traditional property-based approach, which lends itself to positive law, such as bailor/bailee relationships, that are grounded in judicial decisions in legal theory.

Overall, Justice Gorsuch concludes that the *Katz* "reasonable expectations of privacy" test is a supplementary precedential tool available to argue for Fourth Amendment protections and should be used alongside the traditional property-based analysis to "vindicate the full protections of the Fourth Amendment."[19]

16. *Id.* at 2262.
17. *Id.*
18. *Id.*
19. *Id.* at 2272.