N.Y.U. Journal of Legislation and Public Policy
QUORUM

BROOKE G. GOTTLIEB

THE FATE OF *CARPENTER V. UNITED STATES* AND GOVERNMENT ACCESS TO HISTORICAL CELL SITE LOCATION INFORMATION

April 3, 2018

Abstract: The Supreme Court of the United States will soon decide *Carpenter v. United States*, a case in which law enforcement acquired historical cell site location information from Timothy Carpenter's cell phone provider to connect Carpenter to a string of robberies. Carpenter argues that the government's conduct constituted a warrantless search in violation of the Fourth Amendment.

This article discusses the historical and legal context preceding Carpenter and the facts and arguments of the case itself. Then, this article recommends that the Court hold that the government's conduct violated the Fourth Amendment based on a combination of *Katz v. United States'* reasonable expectation of privacy test and the sequential approach to Fourth Amendment analysis. In doing so, the Court should focus on the information the government accesses, as opposed to the technology law enforcement uses, given how quickly technology advances. Ultimately, however, this article concludes that whether the government's investigative techniques qualify as a Fourth Amendment search is a question the legislature, not the Court, should answer.

Author: Brooke G. Gottlieb is an Executive Editor and a J.D. candidate, Class of 2019, at N.Y.U. School of Law

Published by the 2017–18 Editorial Board of the N.Y.U. Journal of Legislation and Public Policy.

THE FATE OF *CARPENTER V. UNITED STATES* AND GOVERNMENT ACCESS TO HISTORICAL CELL SITE LOCATION INFORMATION

Brooke G. Gottlieb

INTRODUCTION

As of January 2018, 95% of Americans have a cellphone and 77% of Americans own a smartphone. Over one-in-ten American adults only have smartphones, not traditional home broadband service – meaning smartphones are their primary means of online access at home. Smartphone use is particularly prevalent among younger adults, non-whites, and lower-income Americans.[1] With technological advancements on the rise, the amount of data accessible to law enforcement has increased dramatically, and the cost of obtaining and analyzing such information has declined. When a user turns a cell phone on, the cell phone constantly reports its location to its cellular service provider, who usually stores that location data.[2] Such transmission by an inactive phone occurs, on average, every seven to nine minutes.[3]

[1] *Mobile Fact Sheet*, Pew Research Center (Jan. 31, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

[2] Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 536 (2017), citing *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. & the Law off the S. Comm. on the Judiciary*, 112th Cong. 228 (2011) (statement of the ACLU), https://www.aclu.org/files/assets/senate_hearing_mobile_tracking_may_2011_-_final.pdf (noting that location data is recorded "approximately every seven seconds").

[3] V. Alexander Monteith, *Cell Site Location Information: A Catalyst for Change in Fourth Amendment Jurisprudence*, 27 KAN. J.L. & PUB. POL'Y 82, 84 (2017).

Reflecting on these statistics, three problems are apparent. First, the framers of the Constitution in no way could have anticipated the scope of intrusion that modern surveillance technologies present. Thus, how can the use of such technologies be reconciled with the United States Constitution?[4] Second, is it correct that "our historical expectations of privacy do not change or somehow weaken simply because we now happen to use modern technology to engage in activities in which we have historically maintained protected privacy interests"?[5] Third, phone companies store cell phone data for a multitude of reasons, such as for legal compliance purposes and to build profiles for targeted advertising. But, to what extent do consumers voluntarily consent to this appropriation? Even if the decision to keep certain records lies entirely with a third party, to what extent does the subject of the maintained records have any rights?

Carpenter v. United States, a case in which law enforcement obtained Timothy Carpenter's historical cell site location information (CSLI) from his cell phone provider to link him to a string of robberies, starkly embodies these three concerns.[6] The Supreme Court will determine whether the government must obtain a warrant based on probable cause to acquire an individual's historical cell site location information from wireless providers. All eyes and ears are now on the Court, which has already heard argument on the case, due to the decision's potential impact on digital privacy standards in the United States.

This article begins by explaining the historical and legal context leading up to *Carpenter*, and then turns to the case itself. Ultimately, this article concludes that the Court should maintain the *Katz v. United States* reasonable expectation of privacy test, combined with what Orin Kerr, a law professor at the USC Gould School of Law, refers to as the sequential approach, which assesses whether a government's action constitutes a search by analyzing the action in a series in isolation.[7] In doing so, the Court should conclude that not only did a warrantless search occur, but that it was unreasonable and thus a violation of the Fourth Amendment. The Court's opinion should emphasize the type of information obtained, not the technology used. Nonetheless, in the future, whether the government's investigative techniques qualify as a search pursuant to the Fourth Amendment is a question that the legislature, not the Court, is far better equipped to answer.

[4] Levinson-Waldman, *supra* note 2, at 528.

[5] *Id*. at 529-30, citing United States v. Davis, 785 F.3d 498, 524-25 (11th Cir. 2015) (Rosenbaum, J., concurring).

[6] Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016).

[7] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012).

I. THE HISTORICAL AND LEGAL CONTEXT PRECEDING *CARPENTER V. UNITED STATES*

The framers of the Constitution were in large part motivated by their disdain for Britain's use of writs of assistance and general warrants. Thus, upon ratification of the Fourth Amendment, courts defined a search as a common law trespass.[8] The physical invasion test for a Fourth Amendment search was explicitly rejected almost four decades later, however, in *Katz*. The Court there held that the government's tapping of a public phone booth to listen to Katz's conversations "violated the privacy upon which he [Katz] justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[9]

Following Judge Harlan's concurrence in *Katz*, courts adopted a two-part test to determine whether government conduct constitutes a Fourth Amendment search. First, did the person claiming a Fourth Amendment violation have a subjective expectation of privacy? Second, is this expectation of privacy one society is prepared to recognize as reasonable?[10] In accordance with this test, "[w]arrantless searches are presumptively unreasonable."[11]

In a trio of cases in the 1960s and 1970s, the Supreme Court, at least partially, clarified *Katz*'s reasonable expectation of privacy test when it developed the third-party doctrine, which lies at the heart of both Carpenter's and the government's arguments. The third-party doctrine holds that individuals who voluntarily give information to third parties have no reasonable expectation of privacy in such information. Therefore, the government does not conduct a Fourth Amendment search as to the individual when it accesses the information from the third party.[12]

---

[8] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

[9] Katz v. United States, 389 U.S. 347, 353 (1967).

[10] *Id*. at 361 (Harlan, J., concurring).

[11] Christian Bennardo, Note, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 FORDHAM L. REV. 2385, 2389 (2017), citing Kentucky v. King, 563 U.S. 452, 459 (2011).

[12] Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the Fourth Amendment did not protect Hoffa's "misplaced belief that a person [informant] to whom he voluntarily confides his wrongdoing will not reveal it."); United States v. Miller, 425 U.S. 435, 442 (1976) (holding that Miller did not have any legitimate expectation of privacy in the content of his bank business records because they were "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"); Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that phone companies record the numerical information that telephone users convey to them without any legitimate expectation that the numbers will remain private).

More recently, in 2012 in *United States v. Jones*, Justice Scalia writing for the Court held that the placement of a GPS device without a warrant was a physical intrusion in a constitutionally protected area, namely Jones' effects, with intent to gather information, and thus violated the Fourth Amendment.[13] In his concurrence, Justice Alito argued that the question should be whether the long-term monitoring of the car's movements violated Jones' reasonable expectation of privacy.[14] In response, Justice Sotomayor argued that even short-term monitoring is problematic because a precise record of a person's movements can be generated in such a time frame.[15] She also questioned the viability of the third-party doctrine as technology advances and people reveal more information about themselves to third parties. "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[16]

After *Jones*, if the Court maintains Justice Scalia's rule, tracking a car's location without a physical trespass would not constitute a search, despite any reasonable expectation of privacy. It remains unclear, however, if *Jones* is limited to GPS data. Take historical CSLI, another type of location data that is used to track suspects and is being litigated for the first time before the Supreme Court in *Carpenter*. As a cellular device connects to cell sites, cell service providers, such as Sprint, AT&T, Verizon, and T-Mobile, maintain records of the device's activity. "'[C]ell sites' refer to the towers and electronic communications equipment that are placed throughout the country (comprising a service provider's network) that make cellular communications possible."[17] Cell service providers can construct and store historical CSLI when the device moves throughout a coverage area, connecting from one cell site to another and transmitting data through radio waves, as it makes a phone call, sends or receives a text message, or refreshes an application.[18] In addition, a cell phone constantly transmits data to the nearest cell tower, even when a user is not actively using the phone. Such transmission by an inactive phone occurs, on average, every seven to nine minutes.[19] Arguably, GPS information is more accurate than historical CLSI, although the real issue is not the technology used but rather the information obtained, as the rest of this article will demonstrate.

[13] United States v. Jones, 565 U.S. 400, 407 (2012).
[14] *Id*. at 419 (Alito, J., concurring).
[15] *Id*. at 415 (Sotomayor, J., concurring).
[16] *Id*. at 417-18 (Sotomayor, J., concurring).
[17] Eric Pait, Comment, *Find My Suspect: Tracking People in the Age of Cell Phones*, 2 GEO. L. TECH. REV. 155, 157 (2017).
[18] *Id*.
[19] Monteith, *supra* note 3, at 84.

II. *CARPENTER V. UNITED STATES*

A. Background

Upon the arrest of four men suspected of committing a series of armed robberies at RadioShack and T-Mobile stores in and around Detroit, Michigan in April 2011, police obtained the confession of one of the men, who gave the FBI his cellphone number and the numbers of other participants. The FBI then applied for, and the magistrate judge approved under the Stored Communications Act, three 2703(d) orders to obtain 152 days of transactional records, including historical CLSI, from MetroPCS and seven days of such records from Sprint of the 16 different phone numbers provided.[20]

At trial, based on the historical CSLI obtained, FBI agent Christopher Hess showed that Carpenter's phone was within a half-mile to two miles of the location of each of the robberies around the time of the robberies.[21] The jury convicted Carpenter of six robberies in violation of the Hobbs Act and five violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting the commission of that offense. Carpenter was sentenced to 1,395 months.[22] The Sixth Circuit affirmed, holding that Carpenter did not have a reasonable expectation of privacy in his historical CSLI.[23]

B. Carpenter's Argument

According to Carpenter, the government conducted a warrantless search when it obtained 127 days of his "highly sensitive information" cell phone location records from his cellular service provider.[24] This search not only violated 47 U.S.C. § 222(f), which prohibits service providers from disclosing customers' CSLI without "express prior authorization," but the Fourth Amendment as well.[25]

Although conceding the third-party doctrine to be a valid limitation on Fourth Amendment protection, Carpenter asserts that the doctrine is inapplicable here. His location records are far more revealing and were not conveyed voluntarily in the same manner as the telephonic and banking information obtained in *Smith* and *Miller* were.[26] "Cell phones are indispensable to

[20] 819 F.3d at 884.
[21] *Id*. at 885.
[22] *Id*.
[23] *Id*. at 889-90.
[24] Brief for Petitioner at 10, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).
[25] *Id*. at 11.
[26] *Id*. at 12.

participation in modern society – often required for employment, relied on for personal safety, and increasingly becoming essential medical treatment tools."[27] One does not "knowingly and intentionally," or even reasonably, expect to disseminate his or her "minute-by-minute movements in historical perpetuity" every time one uses a phone.[28]

C. Government's Argument

The government contends that its procurement of the wireless carriers' cell site records was not a Fourth Amendment search of Carpenter in light of the third-party doctrine.[29] Carpenter had no subjective expectation of privacy in his wireless providers' records of the towers used to make his phone calls. Cell phone users are aware that to make a call, they must be within a tower's coverage area and providers not only know the location of its towers but make records of the use of their towers. Even if Carpenter did have a subjective expectation of privacy, this expectation was not objectively reasonable because cell phone users "voluntarily reveal to their providers information about their proximity to cell towers so the providers can connect their calls. Users cannot reasonably expect that the providers will not reveal that business information to the government."[30] The government also refutes Carpenter's sensitivity distinction between location information and the phone number records in *Smith*[31] and the bank records in *Miller*.[32] The third-party doctrine applies when the government seeks information about a suspect from a third-party witness; its application does not depend on what type of information the government acquires, "no matter how revealing or incriminating the evidence may be."[33]

III. RECOMMENDATION FOR THE COURT

Despite the varying academic approaches to the constitutional analysis of government conduct, the *Katz* test, combined with what Orin Kerr refers to as the sequential approach, should remain at the forefront. At each step of government conduct, the Court should ask whether there was a subjective and an objective expectation of privacy in the information obtained. By doing so, the Court will avoid the issues posed by both the mosaic theory, which assesses "government conduct as a collective whole rather than in isolated steps,"[34] and the quantitative

[27] *Id*.
[28] *Id*.
[29] Brief for the United States at 12, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).
[30] *Id*. at 11.
[31] 442 U.S. 735.
[32] 425 U.S. 435.
[33] Brief for the United States, *supra* note 29, at 12.
[34] Kerr, *supra* note 7, at 320.

approach, which subjects a technology to the Fourth Amendment if it is inherently "broad and indiscriminate" in its monitoring, "or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use."[35] Both of these approaches require assessing the length and extent of an investigative technique, which would be far too complex and time consuming given the speed of which technology advances, and is a balancing test that courts are ill-equipped to evaluate.

In order to conclude that Carpenter had a subjective expectation of privacy in his historical CSLI, the Court should distinguish *Carpenter* from prior cases and hold that law enforcement's conduct here is not protected under the third-party doctrine. In doing so, the Court will maintain the probative value of the doctrine and prevent future large investigative gaps that would occur if it were to abolish the doctrine altogether. Both *Smith* and *Miller* were premised on the defendant's knowledge and assumption of the risk that the information he voluntarily revealed could possibly be disclosed to the government.[36] This factor is missing in *Carpenter*; the Court should hold that Carpenter did not voluntarily convey his location information to his cellular service provider because he did not actively and consciously reveal his information as the defendants in *Smith* and *Miller* did. Even if Carpenter must have known that his location was conveyed to make and receive his phone calls as a matter of common knowledge, he likely did not assume the particular risk that his service provider would reveal his CSLI to the government.

One might then argue that creating a society of willful blindness as to how technology is used will not be manageable long term; it has become a common assumption that when individuals use their cellular devices they are followed everywhere on their phone. Nonetheless, the Court should hold that Carpenter had an objective expectation of privacy. Innovations in technology that enable location tracking do not necessarily mean that social convention has changed such that individuals now accept the government gaining access to location information. If this understanding did follow from advances in technology, one might guess that at the current rate of technological developments, individuals will not have any privacy unless they are completely walled off from others. This is neither realistic nor reasonable. Moreover, even if one argues that individuals have in fact accepted location tracking as a matter of social convention for convenience purposes, such as when ordering food deliveries, that does not necessarily mean that individuals have accepted such tracking for government investigations. There is not necessarily a direct

[35] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 102 (2013).

[36] Smith, 442 U.S. at 742; Miller, 425 U.S. at 442.

correlation between acceptance of location tracking for some purposes and acceptance of location tracking for all purposes.

Lastly, law enforcement's conduct was unreasonable. The amount of data stored on a cellular device that one would never carry on one's person without this technology aggravates privacy concerns and weighs heavily in Carpenter's favor. If the Court accepts law enforcement's use of Carpenter's historical CSLI based on the third-party doctrine, what will stop law enforcement in the future from accessing other types of information that one must release to third-party carriers? Individually the information that a cellular device collects through its applications, such as bank statements, health data, and addresses, does not reveal much about an individual. Yet, these different types of data altogether can potentially reveal very intimate details about one's life, more so than the information in one's wallet can, for instance.[37] It is hard to believe that just by using a cell phone, one has voluntarily revealed all this personal information to the government.

Perhaps the government will argue that the Court will never have to deal with such privacy issues given the Electronic Communications Privacy Act; the law distinguishes between the acquisition of metadata, which requires a 2703(d) order, and content, which requires a warrant.[38] But, the distinction between metadata and content is not very clear. "Sophisticated pattern analytics mean that non-content morphs into content, making any formal distinction meaningless. . . . [T]he numbers one dials reveal hobbies, interests, relationships, and beliefs."[39] Further, if the Court were to not rule in Carpenter's favor, courts would experience similar privacy issues that resulted from England's use of general warrants.[40] The Court would in effect be moving closer towards allowing the government to take advantage of the all-encompassing nature of cellular devices and "obtain a general warrant to access each and every American's location at any given time."[41]

The advocated approach will thus not only uphold the valuable third-party doctrine, but also withstand the test of time and further technological evolutions. Instead of focusing on the particular technology law enforcement used, the rule will emphasize the information obtained from law enforcement's

[37] Riley v. California, 134 S. Ct. 2473, 2489 (2014).

[38] 18 U.S.C.A. § 2703(d) (West 2009).

[39] Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 556, 660 (2017).

[40] *See* Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave it Birth*, 85 N.Y.U. L. REV. 905, 912 (2010).

[41] Heather Phillips, Comment, *The "Big Brother" Effect: The Implications of the Unanswered Question in United States v. Jones*, 48 U. PAC. L. REV. 395, 416 (2017).

conduct. It will also guide law enforcement so that it can determine ex ante whether it requires a warrant to conduct a search based on the information it hopes to acquire, as opposed to waiting for a court to determine if a Fourth Amendment violation has occurred after the fact or seeking Congressional approval for the particular technology used. Given that Carpenter had both a subjective and an objective expectation of privacy in his historical CSLI, and that law enforcement acted without a warrant and unreasonably, the Court should hold that law enforcement's conduct constituted an unlawful search under the Fourth Amendment.

IV. FUTURE STEPS TO BALANCE COMPETING PRIVACY AND TECHNOLOGY CONCERNS

Concluding that Carpenter has a reasonable expectation of privacy in his historical CSLI still leaves questions unanswered regarding government acquisition of other similar metadata records that individuals continuously reveal to third parties. Therefore, in the future, as Kerr suggests, three reasons explain why the legislature should be the governing body that modernizes the third-party doctrine.

First, current Fourth Amendment doctrine typically advises that courts remain cautious when dealing with cases involving new technologies; the *Katz* test in practice has had a limited effect on Fourth Amendment law. Courts frequently reject Fourth Amendment protection in the face of advancing technologies unless a property right is involved.[42] Second, those in favor of judicial determinations of privacy law often point to wiretapping law, as established under *Berger v. New York*[43] and *Katz*,[44] as a prime example of the Fourth Amendment's dominance in the face of privacy concerns due to new technology. However, Kerr believes that the connection between the courts and wiretapping law is vastly overstated. Since *Katz*, "only a handful of judicial

[42] *See* Florida v. Riley, 488 U.S. 445, 451 (1989) (holding that warrantless aerial surveillance of homes from public airspace do not constitute a Fourth Amendment search); United States v. White, 401 U.S. 745, 753-54 (1971) (holding that a police informant wearing a wire to record a conversation in a suspect's home does not violate the Fourth Amendment).

[43] 388 U.S. 41 (1967) (holding that New York State's wiretapping statute was unconstitutional for lack of sufficient procedural safeguards).

[44] 389 U.S. 347 (holding that the Fourth Amendment protected Katz's conversations in a phone booth; physical intrusion is not necessary to invoke the Fourth Amendment).

decisions have found that government wiretapping violated the Fourth Amendment." Instead, wiretapping law has remained in large part statutory.[45]

Third, Kerr insists that the legislature is functionally more equipped than courts are to regulate developing technology. The mere context of judicial decisions inhibits clarification of the law and updates of rules as technology develops. By the time a court rules on a particular case, it often ends up incorporating obsolete assumptions of technology, thereby complicating matters in the present and future. For instance, in support of its opinion, the *Katz* Court highlighted the importance of public telephones in private communication. Yet, today public telephones have become in large part replaced by cell phones and cannot be considered as "vital" as they were in 1967. Therefore, "[t]he privacy implications of a rule at one time may be quite different from the implications of the rule at another time."[46] Courts also face an information gap because they do not have the information necessary to understand how a technology in a given case compares to other changing technologies. Legislatures, on the other hand, with the help of experts, can establish encyclopedic rules that can be updated more frequently.[47] "As a result, legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux."[48]

Kerr's third point is particularly convincing. Just because courts can use their judgment to assess the lawfulness of investigative techniques does not mean they should. Congress' failure to act thus far is not a reason to use the courts in perpetuity and is not a sign that Congress is unable to act. After all, it is the legislature that is an institution that is elected by the people and is supposed to represent the people. The open process by which Congress legislates, often considering opinions from experts, the Justice Department, and civil liberties groups, along with the public scrutiny that follows, will help ensure that the rules Congress develops are based off informed debates that balance government, technological, and privacy interests. The American people should continue to press Congress to act; there are too many privacy concerns at stake to remain complacent.

V. CONCLUSION

Ultimately, the issue in *Carpenter* is not can law enforcement search but rather, what does it need to conduct a lawful search? As technology advances,

[45] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and The Case for Caution*, 102 MICH. L. REV. 801, 807 (2004); *see also* 18 U.S.C.A. § 2511 (West 2008).

[46] Kerr, *supra* note 45, at 867.

[47] *Id*. at 807.

[48] *Id*. at 807-08.

law enforcement's ability to search an individual will likely increase and so will technology's value in police investigations. Yet, there should be procedural safeguards in place before searches occur, especially considering the question of voluntariness with respect to the third-party doctrine. Cell phone users' reasonable expectations of privacy should be protected under the Fourth Amendment, regardless of technological changes. *Carpenter* only discusses historical CSLI, but there is much more information inside a cell phone at stake, such as health and financial data, that law enforcement should not be able to obtain without a warrant. The legislature, as opposed to the courts, should thus take charge, delineate law enforcement's capabilities in its investigations, and balance government interests against privacy interests. Considering how quickly technology advances, the legislature is much more informed than the courts are of the technology at issue and the views of the American people. Until Congress acts, courts should follow the *Katz* test, combined with the sequential approach, to require law enforcement to obtain a warrant based on probable cause before accessing historical CLSI.