Fordham Law Review

Volume 92 | Issue 1 Article 5

2023

Confronting *Carpenter*: Rethinking the Third-Party Doctrine and Location Information

Charlie Brownstein
Fordham University School of Law

CONFRONTING *CARPENTER*: RETHINKING THE THIRD-PARTY DOCTRINE AND LOCATION INFORMATION

*Charlie Brownstein**

The third-party doctrine enables law enforcement officers to obtain personal information shared with third parties without a warrant. In an era of highly accessible technology, individuals' location information is consistently being transmitted to third parties. Due to the third-party doctrine, this shared information has been available to law enforcement, without the individual knowing or having an opportunity to challenge this availability. Law enforcement has utilized this doctrine to obtain comprehensive information regarding individuals' whereabouts over long periods of time.

The U.S. Supreme Court recently limited the reach of the third-party doctrine regarding location data held by cellphone providers. However, this limitation lacks clear guidelines for application by lower courts and has since created significant divergence in application. This lack of clarity has a deeply negative impact on individual privacy rights, as it is difficult to predict how lower courts may approach novel types of technology.

This Note proposes creating a bright-line rule under which courts define property interests by determining who has control over location data, rather than who is currently in possession of it. Because an individual user controls the creation of the information, the third-party doctrine is inapplicable. This solution provides much-needed clarity to the current doctrine, creating a more predictable approach that will better protect individual rights and returning to the original meaning of the Fourth Amendment.

* J.D. Candidate, 2024, Fordham University School of Law; B.A., 2021, Lafayette College. I would first like to thank Professor Bruce Green for his feedback and guidance throughout the Note-writing process. I would also like to thank Liz Gudgel and the staff of the *Fordham Law Review* for their dedication and support. Finally, I would like to thank my family, friends, and cats for their love and support.

INTRODUCTION

Rex Hammond drove alone for five hours,[1] something millions of Americans do without a second thought. However, Hammond was not truly alone. Unbeknownst to him, the police were pinging his cellphone, live tracking his location every fifteen minutes for those five hours.[2] With his

1. *See* United States v. Hammond, 996 F.3d 374, 389 (7th Cir. 2021).
2. *See id.*

location information, they were able to track him to a hotel parking lot, follow him for over an hour after he left, and eventually apprehend him.[3] They had no warrant or authorization from a court to do this.[4]

In Hammond's subsequent case, the U.S. Court of Appeals for the Seventh Circuit questioned the distinction between law enforcement physically following a car and pinging someone's private cellphone and secretly tracking their location.[5] The court answered that there is none, stating that law enforcement could not uncover any substantial private information from such tracking over the course of just five hours.[6] Many reasonable cellphone owners would say otherwise, arguing that they are extremely concerned with the location-tracking capabilities of technology.[7]

The Seventh Circuit's logic in *United States v. Hammond*[8] implicated the third-party doctrine. The third-party doctrine provides that an individual has no reasonable expectation of privacy in information shared with third parties.[9] Common third parties in the technology sector include cellphone providers, internet providers, and internet browsing services. This means that essentially every time an individual uses technology, location data—or other personal information—is shared with a third party.[10] In theory, this means that every time a person visits a location, deposits a check, or purchases medication, that information is accessible to law enforcement without a warrant.[11]

Faced with growing privacy concerns spurred by mass technological development, the U.S. Supreme Court has recently placed narrow limitations on the third-party doctrine.[12] In 2018, the Court held in *Carpenter v. United States*[13] that law enforcement officers obtaining a detailed chronicle of an individual's location information from their cellphone provider violated the Fourth Amendment.[14] However, this limitation lacks any significant guidance for lower courts and leaves the third-party doctrine ripe for law enforcement abuse.[15] Particularly in the realm of location privacy, there is an open legal question of whether location data is truly publicly "shared" or

3. *See id.*
4. *See id.* at 381.
5. *See id.* at 390–92.
6. *See id.* at 392.
7. *See* Venky Anant, Lisa Donchak, James Kaplan & Henning Soller, *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY & CO. (Apr. 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative [https://perma.cc/3969-TJVK].
8. 996 F.3d 374 (7th Cir. 2021).
9. *See* United States v. Miller, 425 U.S. 435, 444 (1976); RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD PARTY DOCTRINE 1 (2014).
10. *See infra* Part I.B.
11. *See generally Miller*, 425 U.S. 435 (1976); U.S. Dep't of Just. v. Ricco Jonas, 24 F.4th 718 (1st Cir. 2022); Smith v. Maryland, 442 U.S. 735 (1979).
12. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
13. 138 S. Ct. 2206 (2018).
14. *See id.* at 2220.
15. *See infra* Part II.B.

provided merely as a necessity of cellphone function.[16] Further, this legal uncertainty asks the broader question of whether the government should be permitted to track individuals simply because they elect to carry a cellphone.[17]

This Note will examine the unsuitability of the third-party doctrine's application to location tracking and the failure of *Carpenter v. United States* to properly address it. These issues are critical to confront because the current state of the third-party doctrine leaves significant confusion among lower courts and results in inconsistencies in its application.[18] This uncertainty means that ordinary citizens and law enforcement officers cannot be certain of the legal limitations of location tracking.

Part I of this Note provides background on developments in Fourth Amendment jurisprudence, with a particular eye toward how the Supreme Court has weighed law enforcement interests against civilian privacy interests as technology progresses. It ends with a discussion of *Carpenter*, the landmark case that limited the scope of the third-party doctrine for the first time. Part II discusses the contradictory case law analyzing other forms of location tracking, specifically real-time tracking, tower dumps, and Global Positioning System (GPS) tracking, all of which rely heavily on third-party data. Part II further discusses the consequences and rationales of these approaches and solutions proposed by scholars with the aim of creating a more coherent approach to location privacy. Finally, Part III proposes a bright-line rule to determine whether location data is subject to Fourth Amendment protections, with the aim of ensuring that law enforcement officers and the public can better understand the limitations of location tracking.

I. THE IMPACT OF TECHNOLOGY ON FOURTH AMENDMENT JURISPRUDENCE

This part provides an overview of Fourth Amendment jurisprudence and how it led to the creation of the third-party doctrine. Sections A and B discuss the original application of the Fourth and Fifth Amendments, as well as how technology has made this original application more complex. Section C discusses the current test that the Court uses when examining Fourth Amendment search cases and the subsequent application of that test. Section D introduces the origin of the third-party doctrine and the complications associated with it. Section E discusses how the Court has confronted technology in the twenty-first century with respect to the Fourth Amendment.

---

16. *See* Laura K. Donohue, *Functional Equivalence and Residual Rights Post-*Carpenter*: Framing a Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 400 (2018).

17. *See* Nathan Freed Wessler, *The U.S. Government Is Secretly Using Cell Phone Location Data to Track Us. We're Suing.*, ACLU (Dec. 2, 2020), https://www.aclu.org/news/immigrants-rights/the-u-s-government-is-secretly-using-cell-phone-location-data-to-track-us-were-suing [https://perma.cc/JG48-NF5V].

18. *See generally infra* Part II.

Finally, Section F introduces the most recent Supreme Court development regarding the third-party doctrine and examines the impacts of this decision.

A. The Original Meaning of the Fourth and Fifth Amendments

The Fourth Amendment protects persons, houses, papers, and effects against *unreasonable* searches and seizures.[19] It is directly tied to the English invasion of the homes of American colonists.[20] At the time of English control over the United States, English authorities authorized the search of all homes to seize prohibited goods under "general warrants."[21] The drafters of the Fourth Amendment strongly opposed these warrants and unambiguously expressed their intent to eliminate them.[22] The Fourth Amendment, in turn, requires that government officials have a warrant before they can perform an unreasonable search or seizure.[23] The warrant must be supported by probable cause and be sufficiently particular.[24] The historical context of the Fourth Amendment elucidates its purpose, which is to prevent unrestricted searches.[25]

Searches in 1791, the year the Fourth Amendment was ratified, looked very different than they do today.[26] The Fourth Amendment's protection was limited to what could be seen by the naked eye or heard directly with the ear.[27] These restrictions explain why the Fourth Amendment's language is expressly aimed at preventing invasions of tangible possessions.[28]

However, less than a century after the Fourth Amendment's ratification, the Supreme Court understood that the invasion of tangible property was not the specific evil that the Fourth Amendment sought to prevent.[29] Rather, the Court believed that the Fourth Amendment was designed to protect the right of personal security, liberty, and property.[30] This liberal outlook on the Fourth Amendment did not last, and later cases increasingly tied its

---

19. *See generally* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

20. *See* Laura K. Donohue, *The Original Fourth Amendment*, 38 U. CHI. L. REV. 1181, 1194 (2016); *Amdt4.2 Historical Background on the Fourth Amendment*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4-1/ALDE_00013706 [https://perma.cc/MT9G-4ATB] (last visited Sept. 3, 2023).

21. *See Amdt4.2 Historical Background on the Fourth Amendment*, *supra* note 20.

22. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1046 (2011).

23. *See* U.S. CONST. amend. IV.

24. *See id.*

25. *See* Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/news/privacy-technology/what-founders-would-say-about-cellphone-surveillance [https://perma.cc/9R9E-3A4U].

26. *See* Steven C. Douse, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J.L. REFORM 154, 158–59 (1972).

27. *See id.* at 159.

28. *See id.*

29. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

30. *See id.*

protections to personal property rights.[31] In the early 1900s, the Court advanced the trespass theory, under which the Fourth Amendment could be triggered only by a physical invasion of private property, search or seizure of a person, or seizure of material possessions.[32] Therefore, activities such as unwarranted wiretapping that did not require *physical* trespass were not included within the meaning of the Fourth Amendment.[33]

The Fifth Amendment was drafted at the same time as the Fourth Amendment, with the same goal of preventing what colonists perceived to be injustices committed by the English.[34] The Fifth Amendment provides five rights; relevant for this Note is the right against self-incrimination.[35] This right, in essence, means that one cannot be compelled to give testimony against themselves in a criminal case.[36]

"Testimony" is oral or written evidence provided by a witness under oath.[37] Testimony is often obtained through a subpoena, which is a legal order to appear in court and testify or produce documents.[38] Individuals named in subpoenas are permitted to invoke the Fifth Amendment if the act of production would be self-incriminating.[39] Critically, however, this ability does not extend to a third party subpoenaed for information about an individual, and there is no basis for the individual to assert a Fifth Amendment privilege if they are not the one compelled to produce the information.[40] This leaves individuals with few defenses when a subpoena is issued to a third party that holds information about them.[41]

There are few legal grounds on which an individual can challenge a subpoena. The Federal Rules of Criminal Procedure (the "Rules") provide that subpoenas may order a witness to produce any documents, data, or objects, but they do not set limitations on the scope of these demands.[42] The Rules establish that a person subpoenaed may move to quash or modify the

---

31. *See* Douse, *supra* note 26, at 162.

32. *See* David P. Miraldi, *The Relationship Between Trespass and Fourth Amendment Protection After* Katz v. United States, 38 OHIO ST. L.J. 709, 711 (1977); Olmstead v. United States, 277 U.S. 438, 466 (1928).

33. *See Olmstead*, 277 U.S. at 466.

34. *See* Dahlia Lithwick, *Where Did the Fifth Amendment Come From?*, SLATE (Feb. 12, 2002, 3:36 PM), https://slate.com/news-and-politics/2002/02/where-did-the-fifth-amendment-come-from.html [https://perma.cc/NSM8-BN3F].

35. *See* U.S. CONST. amend. V.

36. *See* Jennifer Peltz, *Donald Trump 'Took the Fifth.' What Does it Actually Mean?*, AP NEWS (Aug. 10, 2022), https://apnews.com/article/what-does-pleading-the-fifth-mean-0d24abd45972cd80f82f95e4a8eec225 [https://perma.cc/DH9E-Q9JP].

37. *See Testimony*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/testimony [https://perma.cc/8EQU-MV9D] (Apr. 2022).

38. *See* Simeon D. Rapoport, *What Is a Subpoena?*, OR. ST. BAR (Jan. 2016), https://www.osbar.org/public/legalinfo/1062_subpoena.htm [https://perma.cc/VJU7-YVY5].

39. *See* Fisher v. United States, 425 U.S. 391, 409–11 (1976).

40. *See* Orin Kerr, *Does* Carpenter *Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/XP7M-WQZJ].

41. *See id.*

42. *See* FED. R. CRIM. P. 17(c)(1).

subpoena.[43] However, they do not offer standards for such a motion beyond "unreasonable or oppressive."[44] The Court in *United States v. Nixon*[45] offered more substantive limitations to what subpoenas may compel.[46] The Court determined that when issuing a subpoena, the government must prove (1) relevancy, (2) admissibility, and (3) specificity.[47] Without the Fifth Amendment acting as a shield against subpoenas issued to third parties, the Fourth Amendment is typically the only grounds on which a defendant may challenge a seizure of their information stored by a third party.

B. The Growing Influence of Technology and Its Implications on Privacy

The technological landscape in 1791 differs significantly from the one in 2022. The first computer was invented in the mid-1940s,[48] and there was no internet until the 1980s.[49] The first cellphone was sold in 1973,[50] and the first iPhone was released a mere fifteen years ago.[51] All of these devices are now pervasive parts of daily life.

Smartphones likely contain more information about an individual than is known by their closest friends and family, prompting the moniker "spy phones."[52] Smartphones know where a user has gone, whom they have met, what they have purchased, and so much more.[53] A smartphone holds enough information to essentially allow an exact clone of its user to be replicated.[54]

Cellphone carriers, the companies providing mobile connection to smartphones, also have access to historical location data that they are legally

---

43. *See id.* 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive.").

44. *See id.*

45. 418 U.S. 683 (1974).

46. *See generally* United States v. Nixon, 418 U.S. 683 (1974).

47. *See id.* at 700.

48. *See* Erica K. Brockmeier, *The World's First General Purpose Computer Turns 75*, *Penn Today* (Feb. 11, 2021), https://penntoday.upenn.edu/news/worlds-first-general-purpose-computer-turns-75 [https://perma.cc/M3E3-FFT2].

49. *See* Caitlin McLean, *When Was the Internet Invented? What to Know About the Creators of It and More*, USA TODAY (Aug. 28, 2022, 6:00 AM), https://www.usatoday.com/story/tech/2022/08/28/when-was-internet-created-who-invented-it/10268999002/ [https://perma.cc/9ZXZ-47WD].

50. *See* William E. Gibson, *First Cellular Phone Call Was Made 45 Years Ago*, AM. ASS'N RETIRED PERS. (Apr. 3, 2018), https://www.aarp.org/politics-society/history/info-2018/first-cell-phone-call.html [https://perma.cc/BN79-3DWR].

51. *See* Ben Gilbert & Sarah Jackson, *Steve Jobs Unveiled the First iPhone 16 Years Ago—Look How Primitive It Seems Today*, BUS. INSIDER (Jan. 9, 2023, 1:45 PM), https://www.businessinsider.com/first-phone-anniversary-2016-12 [https://perma.cc/7W3P-VG9R].

52. *See* Patrick May & Troy Wolverton, *Your Smartphone Knows Everything About You, and It Tells Tales*, PHYS (May 1, 2011), https://phys.org/news/2011-05-smartphone-tales.html [https://perma.cc/J79W-9R3X].

53. *See* Aaron Brown, *This Is How Much Your Smartphone Knows About You Right Now*, EXPRESS (May 7, 2016, 9:01 AM), https://www.express.co.uk/life-style/science-technology/667868/Smartphone-Knows-About-You-Tracking [https://perma.cc/7AD8-PYPB].

54. *See id.*

permitted to retain for up to five years.[55] Many applications on smartphones allow GPS tracking, which can pinpoint a location within five to ten feet.[56] Even for cautious individuals that avoid or block location tracking apps, cell site location information (CSLI) is recorded during almost every mobile activity, whether or not an individual is aware of the recording or wishes it to occur.[57] Cellphones search for the best signal and continuously attempt to connect to local cell towers, a process that marks a general location for where a user is at any given moment.[58] Thus, wireless carriers such as AT&T and Verizon have comprehensive information about users' whereabouts over long periods of time.[59]

Other devices regularly track an individual in less obvious ways. Internet service providers can see every domain (or website) visited and at what time, painting a vivid image of what a person's preferences, inquiries, and habits look like.[60] Browsing services are no different. Google tracks search history, location, ads viewed, videos watched, and much more.[61] These services are not "tangible" pieces of property but often reveal much more about an individual than a physical object ever could.[62]

The number of Americans implicated in this data-tracking is astounding. Eighty-five percent of Americans own a smartphone.[63] Only 24 percent of these individuals regularly turn their cellphones off, and 92 percent carry their cellphones with them almost everywhere they go.[64] Thus, cellphones have been given all the access needed to record intimate details about a user's

---

55. *See* Rob Pegoraro, *Here's How Long Your Wireless Carrier Holds on to Your Location Data*, PC MAG (Aug. 29, 2022), https://www.pcmag.com/news/heres-how-long-your-wireless-carrier-holds-on-to-your-location-data [https://perma.cc/E7U7-QNL2].

56. *See Mobile Location Data and Covid-19: Q&A*, HU. RTS. WATCH (May 13, 2020, 12:01 AM), https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa [https://perma.cc/E7U7-QNL2].

57. *See* Timothy Tobin, James Denvil & Shee Shee Jin, *U.S. Supreme Court Holds that Historical Cell Site Location Data Is Subject to a Reasonable Expectation of Privacy*, HOGAN LOVELLS LLP (June 26, 2018), https://www.engage.hoganlovells.com/knowledgeservices/news/us-supreme-court-holds-that-historical-cell-site-location-data-is-subject-to-a-reasonable-expectation-of-privacy [https://perma.cc/7Z2M-2H3W].

58. *See* Marguerite Reardon, *Don't Let Your Smartphone Track You*, CNET (June 1, 2019, 5:00 AM), https://www.cnet.com/tech/mobile/dont-let-your-smartphone-track-you/ [https://perma.cc/NB8N-BQJ3].

59. *See* Brian Fung, *Wireless Carriers Keep Your Location Data for Years and Provide It to the Police*, CNN (Aug. 29, 2022, 4:09 PM), https://www.cnn.com/2022/08/29/tech/wireless-carriers-locations-fcc [https://perma.cc/5Y3G-8REC].

60. *See* Darlene Storm, *What Can Your ISP Really See and Know About You?*, COMPUT. WORLD (Mar. 14, 2016, 10:53 AM), https://www.computerworld.com/article/3043490/what-can-your-isp-really-see-and-know-about-you.html [https://perma.cc/R8BR-JWGD].

61. *See* Dave Johnson, *How to Stop Google from Tracking You on any Device*, BUS. INSIDER: REVIEWS (Nov. 27, 2020, 11:34 AM), https://www.businessinsider.com/guides/tech/how-to-stop-google-from-tracking-me [https://perma.cc/L7SU-N5DU].

62. *See* Anant et al., *supra* note 7.

63. *See Mobile Fact Sheet*, PEW RSCH CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/Z3W5-FFUM].

64. *See* Lee Rainie & Kathryn Zickuhr, *Americans' View on Mobile Etiquette*, PEW RSCH. CTR. (Aug. 26, 2015), https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity/#fn-14328-1 [https://perma.cc/GSB5-RN59].

life.[65] These statistics are consistent with internet usage; 93 percent of Americans have broadband internet at home, and only 8 percent do not use it at least once a day.[66]

The American public often endorses the view that technological privacy is crucial.[67] Seventy percent of Americans believe that the privacy of their location is important, and 69 percent feel the same way about their web searches.[68] Although Americans may care deeply about their privacy, that sentiment does not necessarily align with current Fourth Amendment jurisprudence.

C. Fourth Amendment Jurisprudence's Shift Toward Reasonableness

In 1928, the Supreme Court established that the Fourth Amendment is focused on preventing physical trespass.[69] This allowed law enforcement officers to investigate freely so long as there was no physical intrusion onto an individual's property or person.[70] As technology developed, law enforcement officers became capable of discovering significant information without physical trespass.[71] In 1967, the Supreme Court confronted these developments in *Katz v. United States*.[72] Katz was indicted in the U.S. District Court for the Southern District of California for transmitting illegal information over the telephone.[73] To obtain evidence, the police attached an electronic listening device to the telephone booth in which Katz placed the aforementioned calls.[74] The case was brought to the Supreme Court, which held that such a search violated Katz's Fourth Amendment rights.[75]

The majority, expressly departing from the Court's prior view on trespass, held that the Fourth Amendment protects "people, not places" and that its applicability "cannot turn upon the presence or absence of a physical intrusion."[76] Thus, the lack of physical trespass was no longer a determinative factor in whether a search had occurred.

However, courts applying *Katz* in subsequent cases have drawn upon Justice John Marshall Harlan II's concurrence, which created a two-pronged test to determine whether an individual has a reasonable expectation of

---

65. *See* Brown, *supra* note 53.
66. *See Internet/Broadband Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/4UTF-Q23B]; Andrew Perrin & Sara Atske, *About Three-in-Ten Adults Say They are 'Almost Constantly' Online*, PEW RSCH. CTR. (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/ [https://perma.cc/L6K4-ST9U].
67. *See* Rainie et al., *supra* note 64.
68. *See* Anant et al., *supra* note 7.
69. *See generally* Olmstead v. United States, 277 U.S. 438 (1928).
70. *See generally id.*
71. *See generally* Katz v. United States, 389 U.S. 347 (1967).
72. 389 U.S. 347 (1967).
73. *See id.* at 348.
74. *See id.* at 352.
75. *See id.* at 358–59.
76. *Id.* at 353.

privacy.[77] Justice Harlan interpreted prior decisions to require "first that a person . . . exhibit[] an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[78] Justice Harlan used this rationale to differentiate between a conversation held in the home and a conversation held outside, within earshot of outsiders.[79] He reasoned that in the latter situation there is no demonstrated intent to keep the conversation private.[80] Thus, Fourth Amendment analyses began to hinge on the concept of expected privacy, rather than trespass.

Scholars were optimistic that the *Katz* decision would expand the protections offered by the Fourth Amendment; this result was not completely realized.[81] Lower courts applied the test in differing ways. For example, one court found that if a defendant had a reason to believe that the government was routinely surveilling their neighborhood, they could no longer contend that they had an expectation of privacy in their backyard.[82] Other courts held the opposite, finding that advance notice of college dorm searches was insufficient to mitigate privacy interests.[83] Scholars found these differing results troublesome, as they indicated a fatal flaw in the test: it left unclear whether knowledge of diminished privacy amounted to a justification of diminished privacy.[84]

The critiques of *Katz* have only grown as its application continues. Some academics argue that it did very little to replace the trespass standard.[85] The test requires a traditional notion of privacy to be applied, in which the central inquiry is whether privacy can be expected at a specific, physical point.[86] Those academics who believe that *Katz* replaced the trespass standard suggest that the test is meant to focus on the content of the information being monitored, not the means by which the monitoring occurred.[87] However, the language is ambiguous enough to allow either interpretation to be applied.[88]

The Court has expressed concern about the workability of the *Katz* test. In *Kyllo v. United States*,[89] law enforcement officers used a thermal sensor to

77. *See* Erik Luna, *The* Katz *Jury*, 41 U.C. DAVIS L. REV. 839, 842 (2008).

78. *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

79. *See id.*

80. *See id.* ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.").

81. *See* Note, *Reconsideration of the* Katz *Expectation of Privacy Test*, 76 MICH. L. REV. 154, 154 (1977).

82. *See* People v. Superior Ct. (Stroud), 37 Cal. App. 3d 836, 840 (1974).

83. *See* Commonwealth v. McCloskey, 272 A.2d. 271, 273 (Pa. Super. Ct. 1970).

84. *See* Note, *supra* note 81, at 160.

85. *See* Peter Winn, Katz *and the Origins of the 'Reasonable Expectation of Privacy' Test*, 40 MCGEORGE L. REV. 1, 8 (2016).

86. *See id.*

87. *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L. J. 1303, 1306 (2002).

88. *See id.* at 1357.

89. 533 U.S. 27 (2001).

determine the temperature inside a defendant's home.[90] In the resulting decision, Justice Antonin Scalia acknowledged that *Katz* was a circular test but said that its application was most workable when the information could not have been discovered without an intrusion into the home, a constitutionally protected area.[91] This lends credence to both arguments, as it indicates that *Katz* is best applied when a constitutionally protected place is involved, but the result of the search—rather than the method—is what determines its constitutionality.

Two cases decided twenty-nine years apart suggest that physical trespass remains a key part of Fourth Amendment jurisprudence.[92] In *United States v. Knotts*,[93] decided in 1983, law enforcement officers requested that a chemical sales company place a location-tracking beeper onto a drum of chloroform being purchased by Knotts.[94] Knotts drove back to his home, where police subsequently utilized the location sent by the beeper to obtain a search warrant.[95]

On review, the Court held that a person lacks a reasonable expectation of privacy in a vehicle because (1) it is usually a mode of transportation, not a repository for personal items, and (2) it typically travels through public areas where it is in plain view.[96] The Court ultimately concluded that because all of the information provided by the beeper could have been ascertained through visual observations, there was no search conducted under the *Katz* test.[97]

Three decades later, the Court reached the opposite conclusion in *United States v. Jones*.[98] Jones was suspected of trafficking narcotics, and a warrant was issued to install an electronic GPS on Jones's wife's car.[99] Law enforcement officers did not follow the warrant requirements, creating a legally warrantless investigation.[100] The government tracked the vehicle for twenty-eight days and established the vehicle's location within 50–100 feet.[101] At trial, the district court suppressed the data obtained while the vehicle was parked in the garage of Jones's residence[102] but held all other data admissible because a person travelling in a car on public roads has no reasonable expectation of privacy in their movements.[103]

---

90. *See id.* at 30.
91. *See id.* at 34.
92. *See* Caren Myers Morrison, *The Drug Dealer, the Narc, and the Very Tiny Constable: Reflections on* United States v. Jones, 3 CALIF. L. REV. CIRCUIT 113, 118–19 (2012).
93. 460 U.S. 276 (1983).
94. *See id.* at 278.
95. *See id.* at 279.
96. *See id.* at 282.
97. *See id.* at 284–85.
98. 565 U.S. 400 (2012).
99. *See id.* at 403.
100. *See id.*
101. *See id.*
102. *See id.*
103. *See id.*

On review, the Supreme Court held that the government physically occupied Jones's private property when installing the GPS, and that this type of intrusion would have been considered a search at the time of the Fourth Amendment's ratification.[104] The Court enunciated the principle from *Kyllo* that, "[a]t bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[105] The Court contended that *Katz* supplemented the trespass standard of the Fourth Amendment but did not replace it.[106] The Court critiqued the use of *Katz* as an exclusive test, as Jones may not have had a reasonable expectation of privacy in his vehicle's movements.[107] Thus, in this case, solely using the *Katz* analysis may have permitted an unconstitutional search.[108]

Justice Sotomayor concurred, agreeing that a search under the Fourth Amendment occurs when the government intrudes on a constitutionally protected area.[109] However, she disagreed with the Court about their application of the *Katz* test in regard to non-trespassory searches, arguing that technological advances and surveillance techniques will reshape the way society views privacy expectations.[110] She concluded her concurrence by questioning the applicability of the third-party doctrine to a digital age in which a great deal of personal information is routinely shared with third parties.[111]

The *Jones* decision left open questions regarding future Fourth Amendment application. It was distinguishable from preceding Fourth Amendment decisions, such as *Katz* and *Kyllo*, as the Court did not find GPS tracking to require a warrant, instead holding only that placing the GPS on the car required a warrant.[112] Thus, *Jones* gave lower courts significant leeway to determine when GPS tracking without trespass crossed the line into a search on a case-by-case basis.[113]

Further, the Court's reliance on trespass was a shift away from *Katz* and the following jurisprudence.[114] The majority opinion, in determining whether a search has occurred, proposed first asking if there was any trespass before considering the *Katz* test.[115] Without that caveat, existing case law

---

104. *See id.* at 404–05.

105. *Id.* at 406 (second alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

106. *See id.* at 406–07.

107. *See id.* at 411.

108. *See id.* at 412.

109. *See id.* at 413 (Sotomayor, J., concurring).

110. *See id.* at 415.

111. *See id.* at 417.

112. *See* Fabio Arcila Jr., *GPS Tracking out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 64 (2012).

113. *See id.* at 65.

114. *See* Morrison, *supra* note 92, at 116–20.

115. *See* Sherry F. Colb, *The Supreme Court Decides the GPS Case,* United States v. Jones, *and the Fourth Amendment Evolves: Part Two in a Two-Part Series of Columns*, JUSTIA: VERDICT (Feb. 15, 2012), https://verdict.justia.com/2012/02/15/the-supreme-court-decides-

would likely have permitted GPS tracking, especially in the wake of *Knotts*.[116] By relying on physical trespass, the Court did not engage with how technology may shift reasonable expectations of privacy or how physical trespass may inevitably be unnecessary to obtain large amounts of private information.[117] Thus, although *Jones* seemingly provided more privacy protections, it left many questions unanswered about how Fourth Amendment law could be applied in a progressing world.

D. The Katz *Dilemma: Introducing the Third-Party Doctrine*

The proliferation of third-party sharing created greater complexity in Fourth Amendment jurisprudence. Every time a person picks up a prescription at the pharmacy,[118] makes a deposit at the bank,[119] places a phone call,[120] or uses the internet,[121] information is shared with a third party. Thus, the intersection of the Fourth Amendment and shared information has large implications on personal privacy. After *Katz*, courts were confronted with a pivotal question when evaluating searches involving shared information: whether a person can actually anticipate privacy when information is shared with a third party.[122]

In 1976, the Court heard *United States v. Miller*[123] and confronted the question of what, if any, privacy is maintained in information shared with third parties. Miller was allegedly involved in an illegal distillery operation.[124] Agents from the Bureau of Alcohol, Tobacco and Firearms delivered grand jury subpoenas to banks in which the defendant had accounts, requiring them to produce records of his transactions.[125] The banks complied with the order and did not inform Miller about the disclosure.[126] Miller was subsequently indicted and moved to suppress the bank records.[127] He relied on *Katz* to argue that the documents were merely made available to the bank for a limited purpose, and thus that the government violated the reasonable expectation of privacy Miller maintained in his banking accounts.[128]

---

the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves-2 [https://perma.cc/22X3-S65X].

116. *See* Morrison, *supra* note 92, at 120.

117. *See* Nancy Forster, *Back to the Future:* United States v Jones *Resuscitates Property Law Concepts in Fourth Amendment Jurisprudence*, 42 U. BALT. L. REV. 445, 480–83 (2013).

118. *See generally* U.S. Dep't of Just. v. Ricco Jonas, 24 F.4th 718 (1st Cir. 2022).

119. *See generally* United States v. Miller, 425 U.S. 435 (1976).

120. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

121. *See* Storm, *supra* note 60.

122. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 130 (2015).

123. 425 U.S. 435 (1976).

124. *See id.* at 437.

125. *See id.* at 437–38.

126. *See id.* at 438.

127. *See id.*

128. *See id.* at 442.

The Court held that the government did not intrude on any area in which Miller had a protected Fourth Amendment interest.[129] The Court emphasized *Katz*'s holding that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[130] The majority continued that the bank records were voluntarily provided to the bank and routinely exposed to employees, such that Miller assumed the risk that the documents would be shared with the government.[131]

The Court's final justification in *Miller* emphasized that under prior jurisprudence, the Fourth Amendment does not prohibit obtaining information given to a third party, even if the provider of the information expects that it will only be used for a limited purpose.[132] Thus, under the *Katz* analysis, Miller did not have any reasonable expectation of privacy in his bank records.

The *Miller* holding established that no Fourth Amendment rights are violated when a subpoena for personal documents is issued to a third party, even if a criminal prosecution against the document's owner is pending.[133] The Court expanded this principle three years later in *Smith v. Maryland.*[134] In *Smith*, the police suspected Smith of making threatening phone calls and requested that his telephone company install a pen register at its office to record the numbers dialed from the phone in Smith's home.[135] The company complied, and Smith was subsequently indicted.[136] He entered a pretrial motion to dismiss all fruits derived from the pen register for lack of a warrant.[137]

The Court applied the *Katz* test, reciting that the applicability of the Fourth Amendment depends on whether the defendant can claim a legitimate expectation of privacy.[138] The Court clarified that Smith had no property invasion claim and could only argue that there was a legitimate expectation of privacy in the numbers dialed.[139] The Court distinguished the pen register from the listening device in *Katz* because a pen register does not record any contents of communication, only whether communication has been attempted.[140] The opinion expressed doubt that there is any expectation of privacy with numbers dialed, as people realize that telephone companies facilitate the completion of their calls.[141]

The Court was not persuaded by Smith's argument that he demonstrated privacy through making the calls in a private home because the information

---

129. *See id.* at 440.
130. *Id.* at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
131. *See id.* at 442–43.
132. *See id.* at 443.
133. *See id.* at 444.
134. 442 U.S. 735 (1979).
135. *See id.* at 737.
136. *See id.*
137. *See id.*
138. *See id.* at 740.
139. *See id.* at 741.
140. *See id.*
141. *See id.* at 742.

provided about the number is the same regardless of the location from where it was dialed.[142] Even if Smith personally believed that this information would remain private, "this expectation is not 'one that society is prepared to recognize as "reasonable."'"[143]

Smith thus established that law enforcement officers can request that third parties take affirmative steps to obtain information on a specific individual in addition to requesting routinely recorded information.[144] Following *Smith*, the government was entitled to act as an instigator, requiring a third party to record information that they otherwise would not.[145]

The *Miller* and *Smith* decisions created what is now known as the third-party doctrine.[146] The Court endorsed the premise that once information is shared with a third party, ranging from a bank to a telephone service provider, an individual can no longer claim any expectation of privacy in that information.[147] Cases following in the wake of *Smith* and *Miller* added slight nuance to this principle on the basis of a content versus non-content distinction.[148] For instance, law enforcement officers could not read an email, but they could see who the intended recipient was.[149] But this distinction became increasingly difficult as technology became more complicated in the 2000s. Thirty years after *Miller*, third parties started holding information on nearly every facet of daily life through data voluntarily given by millions of smartphone and internet users.[150] This meant that law enforcement officers could obtain extensive records of an individual's movements and activities, which are likely far more intrusive than a home search without a warrant.[151]

E. The Supreme Court Confronts Technology

These decisions reflected a growing concern that the Supreme Court was ill-equipped to confront emerging technology.[152] However, when it decided *Riley v. California*[153] in 2014, the Court indicated a willingness to acknowledge the unique and invasive attributes of cellphones and apply the Fourth Amendment accordingly. Although this case did not discuss third

142. *See id.*
143. *See id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).
144. *See Recent Decision*, 38 MD. L. REV. 767, 779 (1979).
145. *See id.*
146. John Villasenor, *What You Need to Know About the Third-Party Doctrine*, ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ [https://perma.cc/L3NQ-FY52].
147. *See* THOMPSON II, *supra* note 9.
148. *See id.* at 12.
149. *See id.*
150. *See supra* Part I.B.
151. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. & POL'Y 247, 268 (2016); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
152. *See* Joel Graczyk, *Technology at the Court:* Riley *and* Aereo, MARQ. UNIV. L. SCH. FAC. BLOG (July 10, 2014), https://law.marquette.edu/facultyblog/2014/07/technology-at-the-court-riley-and-aereo/ [https://perma.cc/VPQ7-6F5Q].
153. 573 U.S. 373 (2014).

parties, *Riley* provided insight into how the Court may analyze technological developments and reinterpret precedent in response.

Riley was arrested pursuant to a traffic stop, during which a smartphone was seized from his pants pocket.[154] The arresting officer accessed text messages on Riley's phone that the officer perceived to be indicative of gang activity.[155] Following the arrest, a detective conducted a more extensive search of Riley's phone and found videos and photos of criminal conduct.[156] Riley was charged, partially on the basis of these videos and images.[157] In *Riley*'s companion case, *United States v. Wurie*,[158] officers observed Wurie purchasing narcotics and arrested him.[159] The officers noticed that his flip phone was receiving multiple calls from a number identified as "my house" on the external screen.[160] Officers traced the number to an apartment address, secured a search warrant, and subsequently searched Wurie's home, where they found illegal substances, firearms, and money.[161] Wurie faced multiple charges and moved to suppress the evidence obtained from the search of his house, arguing that it was the fruit of an unconstitutional search of his cellphone.[162] The district court denied his motion.[163]

The Supreme Court began the *Riley* opinion by noting that searching a legally arrested person to find evidence was a well-established exception to the warrant requirement.[164] However, smartphones at the time of this case had only existed for seven years, and the Court recognized that smartphones were capable of revealing significant information about an individual.[165] Thus, the Court determined that searches implicating cellphones are not the same as searches implicating wallets or cigarette packs—requiring the Court to reexamine the limits of a search incident to an arrest.[166]

Ultimately, the Court held that a warrant is required before searching a cellphone incident to an arrest.[167] The Court acknowledged that a mechanical application of the existing Fourth Amendment jurisprudence would justify a cellphone search incident to arrest, but it distinguished these circumstances because digital searches do not involve the risk of evidence being destroyed or danger to officers.[168]

The Court noted that cellphones allow law enforcement officers to discover a more extensive degree of information than a typical physical

154. *See id.* at 379.
155. *See id.*
156. *See id.*
157. *See id.*
158. 728 F.3d 1 (1st Cir. 2013), *aff'd*, Riley v. California, 573 U.S. 373 (2014).
159. *See Riley*, 573 U.S. at 380.
160. *See id.*
161. *See id.* at 381.
162. *See id.*
163. *See id.* at 382.
164. *See id.*
165. *See supra* Part I.B.
166. *See id.*
167. *See id.* at 403.
168. *See id.* at 386.

search would permit.[169] Prior to the widespread use of cellphones, searching a person was a narrow intrusion, as there were physical barriers to carrying around large amounts of comprehensive personal information.[170] Thus, the Court made it clear that a cellphone search requires a warrant.[171]

Riley generally received praise as a pro-privacy case.[172] However, the opinion left many questions unanswered.[173] Particularly, the Court reaffirmed the third-party doctrine, even in the age of greater privacy risks.[174] The opinion only briefly discussed the third-party doctrine, distinguishing *Riley* from *Smith* on the basis that in the former case there was clearly a search, whereas in the latter case the Court found that there was not a search.[175] Professor David Harris argues that the Court seemed conflicted in *Riley*, as the Court wanted to prevent warrantless searches of the numbers dialed in a smartphone but ultimately permitted third parties to obtain and provide the same information to law enforcement officers without a warrant.[176]

Although *Riley* cannot be viewed as the end of the third-party doctrine, it certainly left an imprint on the matter. The Court thoroughly discussed the broad privacy issues implicated by cellphones, emphasizing that cellphones essentially document the entirety of one's life.[177] The Court's acknowledgment of these privacy issues left some hope that in the wake of such a pro-privacy majority opinion, the Court was open to revisiting the third-party doctrine.[178]

F. The Limits of the Third-Party Doctrine

The hope that *Riley* marked the beginning of the end for the third-party doctrine may have been justified. Although the third-party doctrine remains alive and well today,[179] *Carpenter v United States*,[180] which was decided four years after *Riley*, limited *Riley's* reach for the first time. In *Carpenter*, prosecutors applied for court orders under the Stored Communications Act[181]

169. *See id.*
170. *See id.* at 393–95.
171. *See id.* at 401.
172. *See Fourth Amendment—Search and Seizure—Searching Cell Phones Incident to Arrest*—Riley v. California, 128 HARV. L. REV. 251, 255 (2014).
173. *See* Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v**.** California, 2014 CATO SUP. CT. REV. 307, 328.
174. *See* Zachary Goldman, Riley v. California—*An Important Step Forward, but How Far Forward?*, JUST SEC. (July 1, 2014), https://www.justsecurity.org/12435/riley-v-california-important-step-forward-forward/ [https://perma.cc/K4WY-U4G9].
175. *See* David A. Harris, Riley v. California *and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PITT. J. CONST. L. 895, 922–23 (2016).
176. *See id.* at 923.
177. *See id.*
178. *See* Marley Degner, Riley *and the Third-Party Doctrine*, WESTLAW J. COMPUT. & INTERNET, Apr. 9, 2015, at 5.
179. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
180. 138 S. Ct. 2206 (2018).
181. 18 U.S.C. § 2703(d).

to obtain CSLI records for the defendant, Timothy Carpenter.[182] The Stored Communications Act allows the government to compel disclosure of certain telecommunications records when the records are relevant and material to a criminal investigation.[183]

Magistrate judges issued orders directing Carpenter's wireless carriers to disclose CSLI for his telephone at call origination and termination sites over a four-month period.[184] This data revealed more than 12,000 location points, an average of more than 100 per day.[185] At trial, a Federal Bureau of Investigation (FBI) Agent testified as an expert about the cell-site data, explaining that each time a cellphone taps into the wireless network, the carrier logs a time-stamped record of the cell site.[186] With this information the FBI Agent was able to produce a detailed map linking Carpenter to four robberies.[187]

Prior to trial, Carpenter moved to suppress the CSLI, arguing that its disclosure was a violation of the Fourth Amendment.[188] His motion was denied.[189] The U.S. Court of Appeals for the Sixth Circuit affirmed, finding that he lacked a reasonable expectation of privacy because he had voluntarily shared his cell-site information with the wireless carriers as a means of establishing communication; thus, that information was not entitled to Fourth Amendment protection.[190]

The Supreme Court overturned the decision. The Court reiterated that Fourth Amendment analysis continues to be guided by an understanding of what was considered to be an unreasonable search or seizure at the time of its adoption.[191] Two main guideposts are that (1) the Fourth Amendment seeks to secure private aspects of life from arbitrary powers and (2) a central aim of the framers was to prevent police surveillance from becoming too intrusive.[192] With these principles in mind, the Court held that Carpenter had an expectation of privacy in his CLSI data.[193] This decision made clear that the Court is not entirely bound to old doctrines if following them would put constitutional law at odds with the digital age.[194]

The Court primarily relied on *Jones*, finding that the tracking used in this case was similar to the GPS device placed on Jones's car, as both provided a "detailed, encyclopedic, and effortlessly compiled" chronicle of location

182. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
183. 18 U.S.C. § 2703(d).
184. *See Carpenter*, 138 S. Ct. at 2212.
185. *See id.*
186. *See id.*
187. *See id.* at 2213.
188. *See id.* at 2212.
189. *See id.*
190. *See id.* at 2213.
191. *See id.* at 2213–14.
192. *See id.* at 2214.
193. *See id.* at 2220.
194. *See* Michael Price, Carpenter v. United States *and the Future Fourth Amendment*, CHAMPION, June 2018, at 51.

data.[195] The Court had already recognized in *Katz* that one does not forgo all Fourth Amendment protections by venturing into a public space.[196] *Jones* furthered that principle by holding that individuals can reasonably expect law enforcement officers to not secretly catalog their every movement for an extended period of time.[197] *Carpenter* completed this line of thinking: to allow the government to access CSLI data would destroy that expectation, and the fact that records are generated for commercial purposes cannot negate privacy expectations in physical location.[198] The data revealed during long-term location tracking provides a window into the "familial, political, professional, religious, and sexual associations" of an individual.[199] The Court also echoed *Riley*'s emphasis that cellphones are essentially part of a human's body now, tracking all of its movements.[200] Location data is logged for almost all cellphone users, so police would not even need to know in advance if a particular person was under suspicion in order to retroactively gain access to a chronicle of their movements.[201]

Carpenter implicated the third-party doctrine because the wireless carriers that held Carpenter's CSLI are considered third parties.[202] Thus, the Court needed to justify not extending *Miller* and *Smith*, under which the search would have been valid. To do so, it first noted that there had been a "seismic" shift in digital technology and that the limited information in the aforementioned cases is incomparable to the huge quantity of data collected by cellphone companies.[203] The opinion continued that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely,'" and *Smith* and *Miller* both considered the nature of the information sought in their determinations.[204] Moreover, there is no affirmative act needed on the part of the user to share their location with the wireless provider; it happens automatically.[205] Therefore, the user is not assuming the risk of sharing their information.[206]

Carpenter marked a movement away from the third-party doctrine but resisted going too far. The Court cautioned that the holding was narrow and applied only to this form of location tracking.[207] More importantly, the Court emphasized that this decision did not overturn the third-party doctrine.[208]

---

195. *See Carpenter*, 138 S. Ct. at 2216.
196. *See id.* at 2217 (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)).
197. *See id.* (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).
198. *See id.*
199. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
200. *See id.* at 2218 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
201. *See id.*
202. *See id.* at 2214, 2216.
203. *See id.* at 2219.
204. *See id.* (quoting Riley v. California, 573 U.S. 373, 392 (2014)).
205. *See id.* at 2220.
206. *See id.*
207. *See id.*
208. *See id.*

The majority explained that they were treading narrowly so as to not "embarrass the future."[209]

Justice Gorsuch dissented, acknowledging the increased privacy concerns surrounding internet usage and suggesting a new approach to interpreting the Fourth Amendment.[210] He explained that under the original meaning of the Fourth Amendment, all that was needed to trigger its protections was the fact that "a house, paper or effect was *yours* under law."[211] He wrote that this approach would not allow for the third-party doctrine loophole, as *Smith* and *Miller* were justified by the *Katz* test and, under an originalist approach, individuals' private information would not become public merely because it is shared with third parties.[212] He supported this through the historical use of bailment, under which property was shared with another for a limited purpose without property rights being lost.[213]

Justice Gorsuch concluded that Carpenter lacked a Fourth Amendment interest in the CSLI under the *Katz* test.[214] He caveated this, explaining that if Carpenter had brought up a positive law argument, one based in property law, Carpenter may have had a claim under the Fourth Amendment.[215] Justice Gorsuch suggested that Carpenter could have relied on federal or state law to argue that legislation protected his property rights to historical CSLI.[216] Likewise, he returned to the theory of bailment, writing that Carpenter could have used prior cases to argue that he maintained property rights even though the information was shared.[217] Therefore, he dissented not because Carpenter did not have a Fourth Amendment interest but because he forfeited a potentially promising argument.[218]

Carpenter limited the third-party doctrine but did not set a clear standard for when lower courts should do the same.[219] The Court provided imprecise factors that provided insights into when information held by third parties was revealing enough to create an expectation of privacy.[220] Suggested factors included: (1) the revealing nature of the information, (2) the comprehensive reach of the information, and (3) the automatic nature of its production.[221] Scholars have subsequently suggested additional factors such as the number of people who would be affected if this collection was permissible, the inescapability of cellphones in modern life, and the low cost of cellphone

209. *See id.* (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
210. *See id.* at 2262 (Gorsuch, J., dissenting).
211. *Id.* at 2268.
212. *See id.*
213. *See id.* at 2269.
214. *See id.* at 2272.
215. *See id.*
216. *See id.*
217. *See id.* at 2268–69.
218. *See id.* at 2272.
219. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 358, 369–70 (2019).
220. *See id.*
221. *See id.*

surveillance compared to traditional surveillance.[222] These factors may have taken *Katz* out of the equation, as the Court provided a normative vision of privacy and set that vision as the standard.[223] Thus, *Carpenter* provided no succinct test to assist lower courts in navigating this groundbreaking decision, while somewhat replacing—or at a minimum supplementing—*Katz*.[224]

This vague rule leaves lower courts with an opening for interpretation.[225] Law enforcement officers have many ways to track location using technology, and *Carpenter* offered guidance on only one: historic CSLI.[226] Thus far, lower courts have been mostly unwilling to extend *Carpenter*'s logic to other forms of tracking.[227] This decision left scholars questioning the future application of *Carpenter* and its potential to implicate other electronic data held by third parties.[228]

II. THE DIVERGENT LEGAL LANDSCAPE IN A POST-*CARPENTER* WORLD

This part will examine the inconsistencies in lower courts' applications of the third-party doctrine to location information and the legal and societal consequences of the resulting confusion. Section A discusses the current critiques leveled against the *Katz* "reasonable expectation of privacy" test and how those critiques have tainted the workability of *Carpenter*. Section B examines lower courts' applications of *Carpenter* to other forms of location information held by third parties. Section C discusses alternate approaches to searches of digital location data, which focus on returning to the text of the Fourth Amendment.

A. The Influence of Katz *on the Legal Issues Surrounding* Carpenter

Katz has been highly criticized for its inability to properly protect privacy interests.[229] In particular, when applying *Katz*, the Court essentially asks one question: whether a person reasonably believes their information will remain private.[230] Professors Susan W. Brenner and Leo L. Clarke argue that the Court in *Miller* and *Smith* fell directly into this one-prong fallacy.[231] They

---

222. *See* Matthew Tokson, *The Impact of* Carpenter v. United States *in the Lower Courts and the Emerging Carpenter Test*, LAWFARE (Nov. 3, 2021, 2:08 PM), https://www.lawfareblog.com/impact-carpenter-v-united-states-lower-courts-and-emerging-carpenter-test [https://perma.cc/7K36-MZ4B].

223. *See* Ohm, *supra* note 219, at 386.

224. *See id.* at 385; Tokson, *supra* note 222.

225. *See infra* Part II.B.

226. *See infra* Part II.

227. Jonathan Cedarbaum, Nina Cahill & Sam McHale, *Digital Data Privacy One Year After* Carpenter, LAW360 (June 20, 2019, 11:06 AM), https://www.law360.com/articles/1170123/digital-data-privacy-one-year-after-carpenter [https://perma.cc/VJD6-TYBX].

228. *See* Ben Barnett, Craig Castiglia & Vernon Francis, *Privacy of Cell Location Data—Analysis of* Carpenter *Decision*, JDSUPRA (July 18, 2018), https://www.jdsupra.com/legalnews/privacy-of-cell-location-data-analysis-57378/ [https://perma.cc/4AW2-6G2D].

229. *See infra* Part I.C.

230. *See* Kerr, *supra* note 122.

231. *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 248 (2006).

state that the Court applied an objective standard when determining that a bank customer has no reasonable expectation that their records will remain private.[232] They suggest that the Court should have instead asked whether it is in society's best interest to protect the bank.[233] These critiques of *Katz* urge the Court to reconsider whether the third-party doctrine is being looked at in the correct context, or whether it should focus on broader societal ramifications of privacy.

The *Katz* test as currently applied creates concerns surrounding equity in the judicial system. Professor Matthew Tokson argues that allowing judges to make determinations about societal expectations leads to inaccurate holdings.[234] Judges and defendants tend to exist in different spheres of knowledge.[235] Judges are often of high socioeconomic status and education levels, whereas defendants accused of criminal activity tend to be low-income individuals of low education levels.[236] This makes individuals implicated in law enforcement surveillance less likely than judges to have knowledge of current methods of surveillance and government programs, meaning that they may be entirely unaware of the capabilities of law enforcement officers to track their location.[237] The *Katz* test, as it is applied, permits judges to presume that defendants have extensive knowledge of novel types of police surveillance and technological tracking.[238]

Even when judges make accurate determinations as to reasonable expectations of privacy, expectations of privacy may shift as society becomes increasingly reliant on technology.[239] The *Katz* test allows these diminished expectations to justify reduced privacy protections in constitutional law.[240] Cases that confront this issue focus on protecting the minimal expectations of privacy that existed at the founding, rather than accepting that modern and founding-era expectations of privacy present very different issues that may require entirely different approaches.[241] The *Carpenter* Court contended that the third-party doctrine, which is predicated on *Katz*, cannot be upheld unconditionally in the face of invasive technology. *Carpenter* seemingly supplemented the *Katz* test with a series of factors, making it important to understand how this hybrid test fits into the critiques leveled against *Katz* and how alternative solutions may formulate a more coherent approach to location-tracking data.

---

232. *See id.*
233. *See id.*
234. *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. L. REV. 139, 169–71 (2016).
235. *See id.* at 169.
236. *See id.* at 170.
237. *See id.*
238. *See id.* at 171.
239. *See* Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013, 1023 (2001).
240. *See id.* at 1025.
241. *See id.*; *see also infra* Part I.B.

B. The Third-Party Doctrine and Location Information in Lower Courts

Carpenter has been critiqued for failing to set sufficient limits on privacy intrusions.[242] Arguably, it failed to truly rethink the third-party doctrine, instead opting to restrict the holding to the "unique" facts of that case.[243] However, in the digital age, *Carpenter* was not truly unique, since numerous forms of technology allow for the same, or potentially more intrusive, surveillance.[244] Following the *Carpenter* decision, numerous lower courts have applied the *Katz-Carpenter* test to various forms of third-party location data, such as tower dumps, real-time CSLI, and car GPSs.

1. Tower Dumps

One type of surveillance in which this critique is well-illustrated are tower dumps. In a tower dump, law enforcement officers request that all wireless providers in a given location provide their cell tower data over a period of time ranging from minutes to hours.[245] This does not target a particular individual, instead targeting a particular location.[246] Law enforcement officers are then provided with a list of all people with cell phones from those providers in that location over the requested time period.[247] In one such instance, law enforcement officers obtained location data on 150,000 individuals, many of whom were not involved in criminal activity.[248] Therefore, although tower dumps do not track an individual in the way that CSLI does, their usage implicates a significantly larger number of people—both those whom law enforcement intended to find and those whom they did not.[249]

The United States District Court for the Northern District of Georgia has held that tower dumps are not implicated by *Carpenter*, and therefore a warrant is not required to execute them.[250] The court found *Carpenter* distinguishable because the information provided through tower dumps does not establish a detailed chronicle of a person's life as the historical CSLI in *Carpenter* did.[251] The court also reasoned that although tower dumps provide information about more people than CSLI does, *Carpenter* did not

---

242. *See* Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contract Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 862 (2022).

243. *Id.* at 862–63.

244. *See id.*

245. *See* Mason Kortz and Christopher Bavitz, *Cell Tower Dumps*, 63 BOS. BAR J. (2019), https://bostonbar.org/journal/cell-tower-dumps/ [https://perma.cc/K2D7-9UJP].

246. *See id.*

247. *See id.*

248. *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 18 (2013).

249. *See id.*

250. *See generally* United States v. Rhodes, No. 19-CR-0073, 2020 WL 9461131 (N.D. Ga. June 18, 2020); United States v. Manning, No. 19-CR-00376, 2021 WL 5236660 (N.D. Ga. Aug. 20, 2021).

251. *See Rhodes*, 2020 WL 9461131 at *2.

invalidate technologies such as surveillance cameras, which present the same issue.[252]

Judge David N. Wecht of the Supreme Court of Pennsylvania, when examining a surveillance technique akin to a tower dump, reached the same conclusion on quite different grounds. Campus safety at Moravian University sought information on who was connected to the campus Wi-Fi in a specific dormitory building while a robbery took place inside.[253] Judge Wecht, in his concurrence, acknowledged that Wi-Fi usage is similar to cellphones' connectivity to a tower, in that it is integrated into almost all parts of daily life.[254] However, unlike cellphones, a person can choose to log off of Wi-Fi at any time.[255] He reasoned that the *Carpenter* holding was partially predicated on the fact that the defendant had no reasonable ability to limit his cellphone's creation of CSLI records.[256] Therefore, if someone does have the ability to prevent the creation of particular records, there would be no reasonable expectation of privacy.[257]

Ultimately, Judge Wecht concluded that Wi-Fi networks could give rise to a reasonable expectation of privacy.[258] However, since connecting to the campus Wi-Fi at any given time was elective, and a user could choose to prevent their location data from being tracked, the court found that there was no reasonable expectation of privacy with Moravian's Wi-Fi network.[259]

These holdings are not consistent across jurisdictions. For instance, in determining whether a tower dump is a search requiring a warrant, the Massachusetts Supreme Judicial Court concluded that tower dumps implicate the same privacy concerns as CSLI because they reveal an individual's location at any given moment.[260] The court relied on the comprehensiveness, the type of information revealed, and the necessity of advanced technology in obtaining the information in reaching this holding.[261] It found that tower dumps, over a period of time, present more of a privacy concern than short-term historical CSLI because they may reveal significant patterns of travel and behavior.[262] Ultimately, the court held that judges must issue warrants for tower dumps.[263]

These divergent applications of *Carpenter* highlight the inconsistencies that the Supreme Court allowed for by not establishing a comprehensive test for the third-party doctrine. Although all of the above courts relied on *Carpenter* and *Katz*, they focused on different factors to reach their holdings, each believing that they were interpreting the case as the Supreme Court

252. *See id.*
253. *See* Commonwealth v. Dunkins, 263 A.3d 247, 251–52 (Pa. 2021).
254. *See id.* at 268 (Wecht, J., concurring).
255. *See id.* at 269–70.
256. *See id.* at 269.
257. *See id.*
258. *See id.* at 271.
259. *See id*.
260. *See* Commonwealth v. Perry, 489 Mass. 436, 452 (2022).
261. *See id.* at 444–46.
262. *See id.* at 451, 453.
263. *See id.* at 462.

required. These inconsistent results are not necessarily an issue; however, the inconsistent reasoning underlying these opinions leave both law enforcement officers and individuals unsure of how privacy should be evaluated.[264]

2. Real-Time CSLI

Real-time CSLI is another type of location tracking, which tracks the live movement of an individual by requiring a wireless carrier to "ping" the individual's phone in order to locate it upon the request of law enforcement officers.[265] Hence, it requires affirmative outreach on the part of law enforcement officers in order to obtain this information.

When applying the *Katz-Carpenter* reasonableness test to real-time CSLI, courts have reached differing conclusions. In *United States v. Hammond*,[266] the Seventh Circuit held that *Carpenter* did not extend to real-time CSLI.[267] In this case, law enforcement officers investigating Hammond, a suspect in a series of robberies, requested that his wireless carrier ping his phone's location so that they could apprehend him.[268] Beginning at 6:00 PM, Hammond's phone was pinged every fifteen minutes until he was stopped around 1:30 AM.[269]

The court compared this technique to the location monitoring undertaken in *Carpenter* and *Knotts*. The court found that it more closely resembled *Knotts*, as the tracking was done over the course of several hours and only collected location data on public roads.[270] This supported the court's holding that no search had taken place.[271] The court reasoned that the CSLI request in *Carpenter* was a search because it was conducted for a period of time sufficient to record Carpenter's private life, whereas the CSLI recorded for Hammond took place over several hours and was thus not as intrusive.[272] Moreover, the court found an "aggravating consideration" in *Carpenter* to be that historical tracking was not something society expected law enforcement officers to be capable of.[273] On the contrary, the government has always been able to track an automobile on a public road.[274] The court in this case did not decide that real-time CSLI could never be a Fourth Amendment

---

264. *See* Wayne R. LaFave, *"Case-by-Case Adjudication" versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 SUP. CT. REV. 127, 141.

265. *See* Shea Denning, *Conducting Surveillance and Collecting Location Data in a Post-*Carpenter *World, Part II*, N.C. CRIM. L. (Oct. 5, 2020, 3:27 PM), https://nccriminallaw.sog.unc.edu/conducting-surveillance-and-collecting-location-data-in-a-post-carpenter-world-part-ii/ [https://perma.cc/RN49-NV6K].

266. 996 F.3d 374 (7th Cir. 2021).

267. *See id.* at 389–90.

268. *See id.* at 381.

269. *See id*.

270. *See id.* at 389.

271. *See id.*

272. *See id.*

273. *See id.* at 390.

274. *See id.*

search such that a warrant is required, rather it clarified that this was a narrow holding specific to the facts presented.[275]

Two years prior, the Texas Court of Criminal Appeals similarly found in *Sims v. State*[276] that real-time CSLI may not require a warrant.[277] Defendant Sims's phone was pinged several times within a three-hour period while he was driving and eventually stopped at a motel.[278]

Although the Texas Court of Criminal Appeals came to the same conclusion as the Seventh Circuit, it did so on very different grounds. The court found that *Carpenter* applied to real-time CSLI and stated that the key question when determining if an action constitutes a search is whether enough information was collected to violate a reasonable expectation of privacy.[279] Since there is no bright line rule for the amount of time that law enforcement officers may track a phone for before they violate a reasonable expectation of privacy, the court stated that it must be determined on a case-by-case basis.[280] In this situation, the three hours of tracking was insufficient to intrude on Sims's privacy.[281]

Contrarily, the Superior Court of Pennsylvania held that collecting real-time CSLI requires a warrant in *Commonwealth v. Pacheco*.[282] Pacheco's phone was pinged in real time on two occasions, once in August 2015 and again in October 2015.[283] The court used two bases of logic from *Carpenter* to establish their ruling: (1) the lack of limitations on CSLI and (2) the fact that the information had not been not voluntarily shared.[284] The court did not find any meaningful difference between real-time and historical CSLI, explaining that just like historical CSLI, "obtaining real-time CSLI is the equivalent of attaching an ankle monitor to the cell phone's user; it allows the government to track the user's every move as it is happening."[285] The court therefore held that obtaining real-time CSLI is a search under the Constitution.[286]

The Supreme Court of Kentucky similarly held that real-time CSLI is never admissible in *Commonwealth v. Reed*.[287] In this case, law enforcement officers pinged Reed's phone for an hour and half until he was apprehended while driving on a public road.[288] The court found the reasoning in *Carpenter* persuasive; like historic CSLI, real-time CSLI is generated

275. *See id.* at 392.
276. 569 S.W.3d 634 (Tex. Crim. App. 2019).
277. *See id.* at 646.
278. *See id.* at 639.
279. *See id.* at 646.
280. *See id.*
281. *See id.*
282. 227 A.3d 358 (Pa. Super. Ct. 2020).
283. *See id.* at 362.
284. *Id.* at 368 (citing Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018)).
285. *See id.* at 370 (citing Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)).
286. *See id.*
287. 647 S.W.3d 237 (Ky. 2022).
288. *See id.* at 242.

without the knowledge or consent of a cellphone owner.[289] The court refused to condone a case-by-case analysis of the constitutionality of a warrantless acquisition of real-time CSLI based on whether a defendant is in a constitutionally protected space such as a home.[290] The court explained that a search that violates the Fourth Amendment is unconstitutional, regardless of the information that it reveals.[291] Thus, in Kentucky, a warrant is required prior to obtaining real-time CSLI.[292]

The aforementioned cases illustrate the different weight afforded to the various factors enunciated in *Carpenter*. Although both the Seventh Circuit and the Texas Court of Criminal Appeals held that the use of real-time CSLI in these particular cases did not amount to a search, the Texas Court of Criminal Appeals specified that the defendant's location did not impact its analysis, whereas the Seventh Circuit found it to be an aggravating factor. Neither court found the involuntariness of the search to be relevant to its analysis, whereas both courts that considered the collection of real-time CSLI to be a search found it particularly persuasive. The courts' varying analyses indicate that the *Carpenter* test has done little to remedy the issues scholars have found with *Katz*.

3. Car Global Positioning Systems

A third type of technology often implicated in law enforcement location tracking are built-in car GPSs. As of 2018, 78 million cars had built-in GPS systems, and it is estimated that 98 percent of new cars sold have them.[293] A car's GPS allows car owners to locate the vehicle if it goes missing or to keep track of people inside the car.[294] Currently, courts apply the *Carpenter-Katz* test to GPS devices, leading to inconsistent holdings under similar fact patterns.[295]

The Texas Court of Appeals held that car GPS data is not subject to protection under the Fourth Amendment. In *LopezGamez v. State*,[296] law enforcement officers were able to obtain the real-time GPS location of a suspect's car from the car dealership.[297] The car was located in a trailer park

289. *See id.* at 247–48.
290. *See id.*
291. *See id.* at 249.
292. *See id.* at 250.
293. *See* Peter Holley, *Big Brother on Wheels: Why Your Car Company May Know More About You Than Your Spouse*, WASH. POST (Jan. 15, 2018, 7:56 PM), https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/ [https://perma.cc/79ZQ-3P39].
294. *See* Jeremy Laukkonen, *What are Car GPS Trackers and How Do They Work?*, LIFEWIRE, https://www.lifewire.com/how-car-gps-trackers-work-4147185 [https://perma.cc/JR32-K9T5] (Sept. 14, 2021).
295. *See generally* LopezGamez v. State, 622 S.W.3d 445 (Tex. Ct. App. 2020) (holding that police obtaining car GPS data did not constitute a search). *But see* United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that obtaining car GPS data constituted a search such that a warrant was required).
296. 622 S.W.3d 445 (Tex. Ct. App. 2020).
297. *See id.* at 451.

in which the defendant and his family lived .[298] The court found that this case did not fit within *Carpenter*'s holding because (1) the defendant allowed the GPS to be installed and (2) the primary purpose of a GPS is to track location, thus one can expect that their movements will be tracked when a GPS device is installed.[299] With these arguments, the court held that the acquisition of the real-time location of the defendant's car was not a Fourth Amendment search requiring a warrant.[300]

In *United States v. Diggs*,[301] the United States District Court for the Northern District of Illinois reached the opposite conclusion. The court held that it is unconstitutional to receive GPS data from a GPS servicer without a warrant. Diggs's wife had signed a contract that allowed for GPS tracking of the vehicle that Diggs was driving when he was suspected of robbery.[302] Upon warrantless request, an employee of the GPS company provided a detective with all location records from the car over the course of a month.[303]

The court found that the privacy issues implicated in this case fit squarely within the reasoning in *Jones* and *Carpenter*.[304] All three cases involved a detailed chronicle of an individual's location.[305] Importantly, here as in *Carpenter*, the officer was able to obtain retroactive data—something otherwise unknowable.[306]

The court rejected the government's assertation that under the third-party doctrine, voluntarily turning information over to a third party forfeits any expectation of privacy.[307] It explained that to hold this would extend the doctrine the same way the Court had declined to in *Carpenter*, as the Court there understood CSLI data to present many of the same qualities as GPS tracking.[308] Thus, the court concluded that the government's acquisition of the historical GPS data constituted a Fourth Amendment search.[309]

These cases illustrate how courts struggle to apply the factors used in *Carpenter* to other forms of location tracking. In both of the above cases, the defendant had explicitly allowed for the installation of a GPS tracker; however, only one court found this determinative in holding that no search had taken place. Contrarily, the Texas Court of Criminal Appeals found this to be irrelevant and insisted that considering it determinative would be doing exactly what the Supreme Court had declined to do in *Carpenter*. Moreover, the Texas Court of Appeals declined to consider the intrusiveness of the information obtained, whereas the Seventh Circuit found the amount of information available to be concerning.

---

298. *See id.*
299. *See id.* at 455.
300. *See id.*
301. 385 F. Supp. 3d 648 (N.D. Ill. 2019).
302. *See id.* at 650.
303. *See id.*
304. *See id.* at 652.
305. *See id.*
306. *See id.*
307. *See id.* at 653.
308. *See id.*
309. *See id.* at 655.

C. A Case for the Return to a Property Approach

Courts' unpredictability in applying *Carpenter*'s holding to various forms of location-tracking data demonstrates that the protections afforded by the Fourth Amendment can be applied differently depending on the state or jurisdiction in which a defendant is tried. Importantly, the current standard fails to provide law enforcement officers and individuals with a clear understanding of their privacy rights—something that is increasingly valued in a digital world.[310] Various scholars have suggested a reimagined textualist approach to the Fourth Amendment when applied to technology.[311]

One proposal argues that the theory of trespass, already expanded on in *Jones*, should be extended further to include trespass onto digital devices.[312] Under this theory, an affirmative act by law enforcement officers to obtain information stored on a private device could be considered "digital" trespass.[313] This approach is somewhat consistent with previous Supreme Court cases; in *Knotts*, the beeper was automatic, not requiring any actions on the part of law enforcement officers to obtain location data.[314] Professor Morgan Cloud, although not proposing a digital trespass theory, suggests that the *Kyllo* holding promoted a "functional equivalent of a trespass."[315] Under this approach, if information could not be accessed without a physical trespass, then accessing it through technology does not make the search constitutional.[316] This more expansive definition of trespass would aim to protect privacy as originally understood at the founding by adjusting its application to meet the increased surveillance abilities of the digital age.

A more popular argument among scholars is that the majority opinion in *Carpenter*—and the third-party doctrine in general—misunderstands the definition of property.[317] Justice Gorsuch broadly suggested in his *Carpenter* dissent that the meaning of property under the third-party doctrine is too narrow in its unjustified rejection of bailment.[318] Professor Laura K. Donohue agrees with Justice Gorsuch's dissent, arguing that CSLI is dependent on the individual who purchases the cellphone, their use of the cellphone, and their movements.[319] Once the purchaser stops using the cellphone or the wireless provider, the provider ceases to have any right to

---

310. *See* Anant et al., *supra* note 7.

311. *See* Morgan Cloud, *Property is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37 (2018); Hannah Cook, *(Digital) Trespass: What's Old is New Again*, 94 DENV. L. REV. F. 1, 7–8 (2017); Donohue, *supra* note 16, at 347.

312. *See generally* Cook, *supra* note 311.

313. *See id.* at 6–7.

314. *See id.* at 6.

315. *See* Cloud, *supra* note 311, at 69–70.

316. *See id.* at 70–71.

317. Donohue, *supra* note 16, at 389; Nicholas A. Kahn-Fogel, *Property, Privacy, and Justice Gorsuch's Expansive Fourth Amendment Originalism*, 43 HARV. J.L. & PUB. POL'Y 425, 467 (2019); Donald L. Buresh, *The Meaning of Justice Gorsuch's Dissent in* Carpenter v. United States, 43 AM. J. TRIAL. ADVOC. 55, 101 (2019).

318. *See* Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting).

319. *See* Donohue, *supra* note 16, at 400.

document that information.[320] She argues that because CSLI is unique to the customer—and its production is entirely dependent on their actions—under a theory of bailment it falls within the definition of property as originally understood.[321] This approach could be extended to other types of location-tracking data, as most are entirely dependent on the user of a device, rather than the provider.[322] Professor Nicholas A. Kahn-Fogel argues that this approach would provide more clarity and avoid the "fruitless quest" of identifying social norms that occurs under the *Katz* approach.[323]

These alternate approaches focus on the text of the Fourth Amendment, moving away from the lack of clarity created by *Katz* and *Carpenter*. Both alternatives protect privacy in the way the founders initially intended,[324] while applying centuries-old law to modern technology. This application would prevent the uncertainties and inequities of the current jurisprudence in a way that promotes privacy rights.

III. REIMAGINING THE THIRD-PARTY DOCTRINE

This part proposes a two-pronged property-based test for determining whether location information shared with a third party can be subpoenaed without a warrant. The proposed test aims to set a clear bright-line rule, remedying the current divergence among lower courts, while protecting the rights of individuals to the highest degree possible under the text of the Constitution. Section A summarizes the flaws in the current test that warrant reinventing a test for the third-party doctrine. Section B explains the proposed test and why it is viable under historical precedent and particularly ripe for adoption given the Supreme Court's current makeup. Section C concludes with several examples of this test applied to the forms of location tracking discussed in Part II.

A. The Gaps Left by Carpenter

Today, the third-party doctrine is in a state of flux.[325] A mere five years ago, this doctrine was a bright-line rule—any data given voluntarily to third parties was available to the government.[326] *Carpenter* held that this is no longer the case and required the government to seek a warrant in order to view certain third-party data.[327] However, the *Carpenter* decision was an exceedingly narrow one, ruling only on historical CSLI data obtained for a period longer than six days.[328] The Court explicitly declined to rule on the various other forms of location tracking, leaving lower courts to decide which personal location-tracking mechanisms could be subject to search protections

320. *See id.*
321. *See id.* at 408–09.
322. *See supra* Part II.B.; *infra* Part III.B.
323. Kahn-Fogel, *supra* note 317, at 474.
324. *See* Cloud, *supra* note 311, at 71; Donohue, *supra* note 16, at 408.
325. *See* Carpenter v. United States, 138 S. Ct. 2206, 2272 (2018).
326. *See* THOMPSON II, *supra* note 9.
327. *See Carpenter* 138 S. Ct. at 2220.
328. *See id.* at 2224 (Kennedy, J., dissenting).

in future cases.[329] By "not embarrassing the future,"[330] the Court has instead embarrassed the present. In an age of rapid technological expansion, the Supreme Court has left ordinary people and law enforcement officers alike with a single opinion that provides limited clarity. Further, information regarding surveillance programs and forms of tracking is most likely to first be disseminated to people of a high socioeconomic class and level of education, the demographic least likely to be impacted by law enforcement surveillance.[331] Under the current framework, those individuals most likely to be the target of this surveillance are also the least likely to have adequate knowledge of it.[332] Courts telling defendants to take steps to prevent surveillance is fruitless when those defendants likely were unaware surveillance was occurring.

Carpenter notably lacks a factor-based test, a bright-line rule, or any qualitative balancing test for lower courts to utilize when facing emerging forms of technology, such as real-time CSLI.[333] *Carpenter* listed a myriad of factors at various points throughout the opinion but never explicitly weighed one as more important than the others, leaving scholars in disagreement on which are even relevant for analysis.[334] The lack of clear direction has enabled lower courts to pick whichever factors they deem most appropriate and exclude unfavorable factors from their analyses entirely.[335] Other lower courts have chosen to bypass the muddled factors, instead comparing *Carpenter* to other Fourth Amendment cases such as *Knotts*, to determine which line of cases aligns more closely with the facts at hand.[336] Although this is not inherently a misuse of precedent, in a time in which digital location tracking occurs regularly,[337] it makes sense to adopt a clear rule on how to determine when a law enforcement officer's request of third-party data encroaches on the constitutional rights of an individual.

Bright-line tests provide a unique degree of specificity and workability for the public and law enforcement officers to understand where individual privacy starts and ends and are particularly well-suited for Fourth

---

329. *See id.* at 2220 (majority opinion).

330. *See id.* (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

331. *See* Tokson, *supra* note 234, at 169–70.

332. *See id.*

333. *See* Ohm, *supra* note 219 ("There is likely to be disagreement about the precise list of *Carpenter* factors, given the wide-ranging nature of the opinion. Different characteristics of CSLI data and smartphone use are emphasized throughout Chief Justice Roberts's opinion.").

334. *See id.*; Tokson, *supra* note 222**;** *see also supra* Part I.F.

335. *See* United States v. Rhodes, No. 19-CR-0073, 2020 WL 9461131 at *2 (N.D. Ga. June 18, 2020) (holding that tower dumps are not searches on the ground that they do not reveal detailed chronicles of one's life); *cf.* Commonwealth v. Dunkins, 263 A.3d 247, 271 (Pa. 2021) (reaching the same result as the U.S. District Court for the Northern District of Georgia on the grounds that the defendant had the ability to avoid the Wi-Fi tower dump).

336. *See* United States v. Hammond, 996 F.3d 374, 389 (7th Cir. 2021).

337. *See* Ned Oliver, *Virginia Police Routinely Use Secret GPS Pings to Track People's Cell Phones*, VA. MERCURY (Apr. 6, 2022, 12:03 AM), https://www.virginiamercury.com/2022/04/06/virginia-police-routinely-use-secret-gps-pings-to-track-peoples-cell-phones/ [https://perma.cc/2YXD-BNF4] (finding that eighteen police departments in Virginia used real-time CSLI to conduct 7,000 days' worth of surveillance in 2020 alone).

Amendment analyses.[338] In *Torres v. Madrid*[339] the Supreme Court held that when law enforcement officers make any form of physical contact with an individual that they intend to restrain—whether or not they are ultimately successful—such contact constitutes a seizure under the Fourth Amendment.[340] This rule provided district courts with a clear, viable reference point to determine when a seizure occurred. *Torres* further displayed that bright-line rules can be useful in defining clear boundaries for law enforcement officers, thus protecting defendants' privacy.[341] Similarly, *Riley* provided a bright-line rule that cellphones cannot be searched incident to arrest.[342] Following this case, courts have been conservative in the leeway extended to law enforcement officers, choosing instead to follow the clear instructions given by the Court that a warrant is required for the search of a cellphone.[343]

In light of privacy concerns, courts should follow the approach in *Riley* and set standards for when it is permissible for the government to subpoena third parties for location information. The need for clarity is especially urgent in a time when individuals are actively concerned about their rights as technology expands to become increasingly invasive.

B. A Return to the Original Meaning of the Fourth Amendment

To best effectuate the purpose and text of the Fourth Amendment, the ultimate test to determine whether subpoenas for third-party location data are unconstitutional should be based on the concepts of property and trespass. As Justice Gorsuch explained in his *Carpenter* dissent, property rights do not dissipate when information is shared with a third party.[344] Therefore, expanding the current judicial understanding of "property" and "trespass" to accommodate for the changing technological landscape will create a workable test and follow the meaning of the Constitution. This test asks two questions, both of which guarantee individuals their constitutional rights in a digital age:

---

338. *See* LaFave, *supra* note 264; *see also* Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001).

339. 141 S. Ct. 989 (2021).

340. *See id.* at 998.

341. *See* Lawrence Hurley, *U.S. Supreme Court Widens Ability to Sue Police for Excessive Force*, REUTERS (Mar. 25, 2021), https://www.reuters.com/article/us-usa-court-police/u-s-supreme-court-widens-ability-to-sue-police-for-excessive-force-idUSKBN2BH2I5 [https://perma.cc/HP76-3BH4]; *see also* Edward R. Alexander, *The Right of Privacy and the New York State Constitution: An Analytical Framework*, 8 TOURO L. REV. 725, 742 (arguing that state courts should utilize bright-line rules to protect constitutional rights).

342. *See* Justin P. Murphy & Louisa K. Marion, Riley v. California*: The Dawn of a New Digital Age of Privacy*, BLOOMBERG L. (July 9, 2014, 4:02 PM), https://news.bloomberglaw.com/e-discovery-and-legal-tech/riley-v-california-the-dawn-of-a-new-digital-age-of-privacy [https://perma.cc/J7K8-UGHA].

343. *See* K. Carrie Sarhangi, Riley *Cellphone Search Rule is Slowly Sweeping the Nation*, LAW360 (Sept. 26, 2014, 10:08 AM), https://www.law360.com/newyork/articles/577356/riley-cellphone-search-rule-is-slowly-sweeping-the-nation [https://perma.cc/58NS-Z4A4].

344. *See* Carpenter v. United States, 138 S. Ct. 2206, 2268–72 (2018) (Gorsuch, J., dissenting).

1. Is the information obtained by law enforcement the property of an individual?

2. If the information does not constitute property, did it require a trespass on property to obtain?

Answering either of these questions in the affirmative would necessitate a warrant in order to preserve the search's constitutionality. Implementation of this test would require a case similar to *Carpenter* to reach the Supreme Court, but Fourth Amendment precedent and the current ideological composition of the Court make this test a likely candidate for majority approval. Since the Court specifically declined to rule on other forms of location tracking, a similarly invasive case using real-time CSLI or extensive tower dump information would be an ideal place for the Court to make the sweeping changes that this test necessitates.

1. The Property Prong

This test's first prong requires changing the current understanding of property from being dependent on possession to dependent on control. In order for this prong to cover any form of location tracking discussed in Part II, the premise of the third-party doctrine enunciated in *Smith* and *Miller*—that voluntarily sharing information with third parties removes all claims of property rights—can no longer stand.[345] The presumption that voluntary sharing destroys one's property interest does not align with existing precedent; papers, including letters that have already been sent and are no longer in an individual's possession, are considered property and cannot be searched without a warrant.[346] Thus, the Court would have to deviate from the current presumption about voluntarily sharing data.[347]

Instead, this property prong would prompt the court to ask the following: if the information was not shared with a third party, would it be considered property? *Riley* offered a clear answer to this question by comparing cellphones to a container. It was not the cellphone itself that justified the warrant requirement, but rather the information stored in it.[348] The ability to access location data, however, has never been predicated on the distinction between property and data generated by that property; rather, it has been predicated on the idea that once data is shared property interests are waived.[349] But if location tracking was accessed directly through a cellphone, it would be a Fourth Amendment violation under *Riley*.[350] This disconnect illustrates a flaw in the assumption that a user is never in possession of their own location data—that it is merely generated by the user

345. *See generally* supra Part I.D.

346. *See Carpenter*, 138 S. Ct. 2206, 2269 (Gorsuch, J., dissenting).

347. *See supra* Part I.F.

348. *See* Riley v. California, 573 U.S. 373, 397 (2014) (explaining that data stored on a cellphone is often stored in a cloud-based server and the search of that data equates to using a key found on an arrested individual to open the door to their home).

349. *See* United States v. Miller, 425 U.S. 435, 440 (1976) (finding that once Miller shared his documents with the bank, he no longer had a property claim over them).

350. *See generally* Riley, 573 U.S. 373.

and in possession of a third party. Accepting Professor Donohue's definition of historical CSLI data as property, the property right belongs to the individual who controls the creation and sharing ability of the information.[351]

The concept and commonality of bailment at the time of the founding may make this concept legally easier to reckon. Bailment is an established legal concept that allows one to maintain property rights, even if possession of the property is always shared with a third party.[352] Justice Gorsuch accepted that this theory of bailment may extend to digital data.[353] Professor Donohue further asserted that bailment does apply to historical CSLI, as the cellphone owner is wholly responsible for the creation of the information, and the cellphone provider only retains the information while permitted to do so by the owner.[354] The long-existing idea that lack of possession and an interest in property are not mutually exclusive provides ample legal support to suggest that data created entirely based on an individual's actions and devices is the property of that individual, even if it is "possessed" by another.

2. The Trespass Prong

The second prong extends the concept of trespass to digital devices. Currently, the third-party doctrine does not consider a third-party's intrusion on an individual's private device for law enforcement purposes to be an act of trespass.[355] The second prong of the proposed approach considers trespass as *ancillary* to property. For instance, certain means of location tracking involve directly accessing the cellphone while it is on an individual's body.[356] Under this prong, this practice should be considered clear trespass, even if it does not involve physically stepping into one's private space. The Supreme Court has addressed similar issues of private digital trespass in employer-employee relations and the limitations of the Computer Fraud and Abuse Act of 1986.[357] In doing so, the Court noted that the common law is deficient in regard to computer crime.[358] Trespass by law enforcement officers under the Fourth Amendment has been understood more broadly than trespass under common law when following the common-law approach would leave individuals vulnerable to privacy intrusions by law enforcement

---

351. *See* Donohue, *supra* note 16, at 409 ("[W]here the underlying data arise from the actions of an individual, and that person has the original legal right to determine whether and with whom it is shared, they hold an ownership interest in it.").

352. *See* David J. Seipp, *The Concept of Property in the Early Common Law*, 12 L. & HIST. REV. 29, 52 (1994).

353. *See* Carpenter v. United States, 138 S. Ct. 2206, 2268–71 (2018) (Gorsuch, J., dissenting).

354. *See* Donohue, *supra* note 16, at 400.

355. *See generally* Sims v. State, 569 S.W.3d 634 (Tex. Crim. App. 2019); United States v. Hammond, 996 F.3d 374 (7th Cir. 2021).

356. *See supra* Part II.B.2. (describing how real-time CSLI involves remotely contacting an individual's phone).

357. 18 U.S.C. § 1030; Van Buren v. United States, 141 S. Ct. 1648, 1655 n.4 (2021).

358. *See Van Buren*, 141 S. Ct. at 1655 n.4.

officers.[359] Thus, even though the common law may not cover this sort of digital trespass, the Supreme Court may elect to do so.

The suggestion that the common law does not adequately cover trespass indicates a willingness of the Court to view trespass onto a digital medium as more akin to a traditional physical trespass. Under constitutional law, law enforcement officers cannot physically access the property of another person without a warrant.[360] Importantly, the Court has already asserted that an individual accessing a computer without authority constitutes an untraditional form of property deprivation.[361] The same standard should be true for law enforcement officers. The Supreme Court's apparent acceptance that digital trespass exists helps bolster the reformed standard of this second prong: when law enforcement, through a third-party, accesses an individual's device, that intrusion constitutes a trespass.

3. Practicability of the Proposed Test

This test requires returning to a more historical understanding of the concept of property and trespass. Like many other historical aspects of the law, these concepts can be adjusted and reimagined to meet the demands of the twenty-first century;[362] these definitions too should be adapted. Both textualists on the Court and justices who are typically more protective of defendants are likely to find unity in this test. Textualists such as Justices Thomas, Alito, and Gorsuch have already made this argument explicitly, criticizing the Court's deviation from the Fourth Amendment's text based on the *Katz* test, arguing that it should once again be predicated on property and trespass.[363] The more defendant-friendly justices, such as Justice Sotomayor, have not gone so far as to name these two concepts but have criticized the third-party doctrine on face value.[364] This test would essentially eliminate the third-party doctrine's applicability to digitally-stored location data based on the text of the Fourth Amendment, providing both "sides" of the Court with common ground.

Justice Gorsuch indicated that he would agree with a test similar to this one. In his *Carpenter* dissent, he stated that he was not convinced Carpenter had property rights in the data.[365] However, he did not entirely preclude the possibility. Rather, he stated that property rights and digital data present complex questions that may be better left to the legislature.[366] Importantly,

---

359. *See* Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. REV. 103, 109–16 (2017) (discussing several Supreme Court cases in which the Court found that law enforcement officers trespassed even though their actions did not constitute trespass under common law).

360. *See* U.S. CONST. amend. IV.

361. *See* Van Buren, 141 S. Ct. at 1648.

362. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); Riley v. California, 573 U.S. 373, 393 (2014).

363. *See Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting); *id.* at 2238 (Thomas, J., dissenting).

364. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

365. *See Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

366. *See id.* at 2270.

he did state that Carpenter's lack of physical or sole possession of his data did not preclude him from asserting a property interest.[367] Justice Gorsuch compared historical CSLI to the theory of bailment, pursuant to which a bailor comes to hold property of another for a specified purpose and still owes a duty to only utilize the property for that purpose.[368] This line of reasoning served as the baseline for the argument that property interests are not lost by incidentally sharing property with another party, but Justice Gorsuch did not provide a working definition of property in the digital age. The test proposed in this Note recognizes property as any data produced by an individual's device or system, even if stored by a third party. This definition applies the well-accepted concept of bailment to modern concerns regarding privacy, providing individuals with more protection and law enforcement officers with clear guidelines.

Finally, a reformed test would provide necessary leeway to lower courts. Although having a bright-line rule has many benefits, it also limits courts' ability to develop a nuanced approach to complicated questions, facts, or changing technology. The definition of property does not have to be static.[369] Under this new test, lower courts are not required to all find the same property interests in each piece of technology or data. Courts may find that the collection of data was not controlled by the individual using a device or service, while other courts may hold the opposite. Section C will examine these nuances further.

This test will likely receive the same critique that many others do: it fails to account for future technologies. However, as *Carpenter* demonstrated, tests do not need to be stagnant or lie untouched for decades. This proposed test can be adjusted and changed to fit an adapting world.[370] If at some point a technology develops that can track location in an alarming manner, the test can be altered in order to better account for that. Under this test, a person owns any data created by a device they own or a system they are using. It is intended to establish broad protections for defendants in a time when they are desperately needed. It is nearly impossible to conceptualize the types of technology that will develop or how AI and the metaverse will change the landscape of law and technology.[371] An adaptable test is better suited than reactive decisions to each unique type of technology or data invasion. Because the Supreme Court hears so few cases each year,[372] such delayed lawmaking is unsuitable protection for defendants subject to invasion by law enforcement.

---

367. *See id.* at 2269.

368. *See id.*

369. *See id.* at 2259 (Alito, J., dissenting) (arguing that Carpenter's cellphone carriers' possession of his CSLI records did not constitute bailment); *cf. id.* at 2269 (Gorsuch, J., dissenting) (suggesting that Carpenter's cellphone carriers' possession of CSLI records could constitute bailment).

370. *See generally id.*; *see also* Riley v. California, 573 U.S. 373 (2014).

371. *See* Thomas Koulopoulos, *This Robot Video Will Show You Why It's So Hard to Predict The Future*, INC. (Dec. 1, 2022), https://www.inc.com/thomas-koulopoulos/this-robot-video-will-show-you-why-its-so-hard-to-predict-future.html [https://perma.cc/4S87-7T9P].

372. *See Supreme Court Statistics*, 135 HARV. L. REV. 491, 498 (2021).

There may be additional concerns levied against the broad protections this test provides and its apparent rejection of the third-party doctrine.[373] However, this test does not prevent law enforcement officers from accessing this information. First, law enforcement officers may obtain a warrant or, in the case of an exigent circumstance, continue without a warrant.[374] They may also subpoena the information directly from the individual who created it. Moreover, the definition of property provided by this test is not a novel definition.[375] Until *Miller* and *Smith*, the idea that sharing information for a limited purpose removes all property interests did not align with precedent. Rather, the precedent suggested that individuals maintained property rights even after information was shared. This adjusted definition of property does not make every piece of data the property of an individual; it assures that information whose creation is dependent on a single individual will remain controlled by that individual. The proposed test aims to increase individual privacy in an age of rapidly developing technological innovation and set clear standards for when third-party sharing that involves sharing an individual's information with law enforcement officers is a search under the Fourth Amendment. It is crucial to understand the proposed test's application to existing technology and how that application may be extended to technology that does not yet exist.

C. Application of the Proposed Test to Current Forms of Location Tracking

1. Tower Dumps

Tower dumps are perhaps the most complex type of information to analyze under this test. As it does not involve any direct access to an individual's device, a tower dump would not be covered under the trespass prong. Lower courts may diverge in determining whether the data collected in tower dumps is property. The definition of property under this test requires an individual to be wholly in control of the creation of the data. Tower dumps involve a compilation of the data of potentially thousands of individuals. Thus, they are not a single person's property.

Tower dumps are not dependent on a singular person's creation. If one person involved in a tower dump stopped using a cellular provider, the tower dump could still occur. The definition of property hinges on who creates the data;[376] although cellphone users in this instance allow the creation of data, the creation of data does not depend entirely on them.[377] Thus, following a strict definition of property, the cellphone provider cannot be considered a "bailee."

---

373. *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573 (2016).

374. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

375. *See id.* at 2268–69 (describing how bailment has historically been accepted by the Court).

376. *See* Donohue, *supra* note 16, at 409; *supra* Part III.B.1.

377. *See supra* Part II.B.1.

The alternative to this would be considering the cellphone provider to be a bailee to every individual who is sharing their information; thus, they would be utilizing each individual's property, and sharing it would require a warrant. Ultimately, it would require a much broader reading of the definition of property to find that tower dumps are implicated. Lower courts may opt to choose this definition in order to better protect the privacy of individuals. However, under the stricter definition this test employs, tower dumps are created by the cellphone provider and not property of the cellphone user.

2. Real-Time CSLI

Real-time CSLI is where this test applies most neatly. In order to obtain real-time CSLI information, a cellphone provider must typically "ping" an individual's cellphone in order to access their location.[378] This process demands that a third party reach out to an individual's property—their phone—without consent to access information that is not available without technology. Under the proposed expanded definition of property, this process is an intrusion onto the property of another party and would qualify as a digital trespass.

A potential counterargument is that third parties are authorized to access real-time CSLI through user consent or cellphone agreements. However, *Carpenter* found that the necessity of owning a cellphone to participate in the modern world requires a more critical analysis of the contractual rights sacrificed in an agreement with cellphone companies or wireless providers.[379] Given that cellphones are almost always carried by their owners, allowing real-time CSLI would give wireless providers the green light to find out where an individual is at any point in their life.[380] Because the *Carpenter* Court already expressly declined to extend this reasoning to historical CSLI due to the extensive tracking capabilities that a cellphone provides,[381] it would make little sense to diverge from the Court's logic for real-time CSLI.

An additional counterargument to this is that the information obtained from real-time CSLI is typically collected when one travels on a public road, and the police are constitutionally permitted to follow someone in a car—implying that the information is not unique and would not typically require advanced technology to obtain.[382] This argument would become irrelevant under the proposed trespass prong. By redefining digital intrusion as akin to physical intrusion, digital devices, as effects of an individual, would receive identical Fourth Amendment protections. If law enforcement officers wish to follow someone on a public road, they may do so, but they may not trespass

---

378. *See* Denning, *supra* note 265.
379. *See Carpenter*, 138 S. Ct. at 2218 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
380. *See Mobile Location Data and Covid-19: Q&A*, *supra* note 56.
381. *See Carpenter*, 138 S. Ct. at 2219.
382. *See* Cook, *supra* note 311, at 7–8; United States v. Jones, 565 U.S. 400, 403 (2012).

on the individual's property to accomplish the same goal; the police are entitled to follow someone on a public road,[383] but they are not entitled to enter that person's car unless they have probable cause to do so.[384] Accessing a cellphone inside a car is analogous to the latter situation. Therefore, accessing an individual's cellphone for real-time CSLI, regardless of where that cellphone is located, constitutes a digital trespass onto the effects of an individual, such that a warrant is required.

3. Car Global Positioning Systems

The application of a new bright-line test to GPS data is more complicated but would likely trigger protection through a revised definition of property invasion. If a person owns a car with a GPS, under this test, any data produced by the GPS would be that person's property. The purpose of a car GPS is generally for the owner of the car to find their car if it is stolen or lost, not to benefit the GPS company.[385] Thus, comparing this purpose to the bailment concept,[386] the data held by a GPS installed in a car is akin to the property of an individual held by a bailee. This analysis does not change when considering cars that are leased or financed; there is no legal exception that allows police to enter a home with a bank's permission if it is mortgaged or a tenant's apartment with the landlord's permission.[387] It would be similarly inappropriate to say that an individual has no property rights over GPS data produced by their car because it is not yet paid in full. Because the creation of location data from a GPS installed in a car is entirely dependent on and controlled by the car owner, a warrant would be required to obtain it.

4. Beyond Location Tracking

Although this proposed test was created for and focuses on location data, there are numerous other types of data created by personal technology that is shared with third parties.[388] Justice Gorsuch already touched on how such a test may entirely overturn *Smith* and *Miller*.[389] Adoption of this test would curtail the third-party doctrine but may not entirely relegate it to the past. There is data on individuals stored by third parties but not created by an individual's use of a device or service, such as pharmacy records to which the third-party doctrine has been applied.[390] When the individual plays no role in the creation of data, and that data is instead created entirely by a third party, the property prong of the test cannot extend that far. It extends to data created by an individual's property containing information on that individual.

---

383. *See Jones*, 565 U.S. at 403.
384. *See* United States v. Ross, 456 U.S. 798, 809 (1982).
385. *See How Do Car Trackers Work?*, PROGRESSIVE, https://www.progressive.com/answers/how-do-car-trackers-work/ [https://perma.cc/5QXX-V5MH] (last visited Sept. 3, 2023).
386. *See supra* Part III.B.1.
387. *See* Chapman v. United States, 365 U.S. 610, 616 (1961).
388. *See* Storm, *supra* note 60; Brown, *supra* note 53.
389. *See* Carpenter v. United States, 138 S. Ct. 2206, 2272 (2018) (Gorsuch, J., dissenting).
390. *See generally* U.S. Dep't of Just. v. Ricco Jonas, 24 F.4th 718 (1st Cir. 2022).

The third-party doctrine will not be completely overturned, but its scope and use will be miniscule.

CONCLUSION

The third-party doctrine allows an individual's information that has been shared with a third party to be given to law enforcement officers without a warrant, whether or not the individual is aware that information has been shared. In the age of digital technology, comprehensive and detailed information regarding an individual's location is unwittingly being shared with third parties. *Carpenter* failed to sufficiently curtail the privacy invasions permitted under the third-party doctrine, instead leaving a convoluted set of factors for lower courts to analyze. This Note argues that the Supreme Court should return to a textualist approach to the Fourth Amendment when applying it to location information held by third parties. This solution will provide a more equitable approach to the third-party doctrine and protect individuals' rights as they were understood at the time of the founding.