Journal of Business & Technology Law

Volume 17 | Issue 2 Article 6

*Carpenter v. United States:*A Systematic Shift in the Fourth Amendment Jurisprudence in the Digital Age

Shelby McCloskey

Carpenter v. United States : A Systematic Shift in the Fourth Amendment Jurisprudence in the Digital Age

SHELBY MCCLOSKEY*©

* J.D. Candidate, 2022, University of Maryland Francis King Carey School of Law. The author would like to thank the editors and staff on the Journal of Business & Technology Law for their feedback and support throughout the writing process. The author would also like to thank her family and friends, especially her parents Matt and Mary McCloskey, for their continued love, support, and encouragement throughout all of her academic endeavors.

Carpenter v. United States

TABLE OF CONTENTS

SHELBY MCCLOSKEY

INTRODUCTION

In today's digital society, determining how to safeguard "[t]he right of the people to be secure in their persons, houses, papers, and effects[] against unreasonable searches and seizures"[1] is becoming increasingly difficult.[2] This is especially true with respect to information provided to third parties.[3] Although the Fourth Amendment protects against government intrusions into areas where "a person has a constitutionally protected reasonable expectation of privacy;"[4] the Fourth Amendment does not protect said intrusions if the government is compelling information that people voluntarily cede to third parties.[5] This concept is now known as the third-party doctrine.[6] Looking at the pervasive, precise, and inescapable nature of modern-day technology, the Court in *Carpenter v. United States*[7] revisited this doctrine to determine when and how it should be applied in today's environment.[8] Specifically, the Court addressed "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[9]

Although, under the third-party doctrine, one usually does not have Fourth Amendment protection in information voluntarily ceded to third parties, the Court "decline[d] to grant the state unrestricted access to a wireless carrier's database of physical location information."[10] Instead, the Court held that "[t]he Government's acquisition of the cell-site records here was a search under that Amendment[,]"[11] triggering the warrant requirement.[12] In doing so, the Court correctly declined to extend the third-party doctrine from *United States v. Miller*[13] and *Smith v.*

1. U.S. CONST. amend. IV.

2. *See infra* Part II.C.

3. *See* Alyssa M. Brumis, *The Right to Privacy in a Digital Age: Reinterpreting the Concept of Personal Privacy*, INQUIRIES J. 8.09 (2016), http://www.inquiriesjournal.com/a?id=1450 (noting that third parties are recording more extensive and precise information through an expansive array of surveillance practices, including through social media, cell phone applications, the internet, GPSs, and more).

4. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

5. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (noting that "[t]his Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [a third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"); *see also infra* Part II.B.

6. *See Miller*, 425 U.S. at 433.

7. 138 S. Ct. 2206 (2018).

8. *Id.* at 2216-17.

9. *Id.* at 2211.

10. *Id.* at 2223.

11. *Id.*

12. *Id.* at 2221.

13. 425 U.S. 435 (1976).

Maryland[14] to cell-site location information ("CSLI").[15] Consequently, the Court correctly identifies a seismic shift in digital technology, but incorrectly fails to reconstruct the third-party doctrine for the digital age.[16] Lastly, the Court's holding that warrants are required when surveillance methods obtain "information [that] is detailed, encyclopedic, and effortlessly compiled"[17] could have negative effects on privacy expectations during the COVID-19 pandemic and could cause confusion amongst the courts both during the global-wide COVID-19 pandemic as well as in its aftermath .[18]

I. THE CASE

In 2011, the FBI arrested four suspects while investigating a string of robberies.[19] One of the arrestees admitted to robbing nine stores and provided the FBI with the cell phone numbers of fifteen (15) accomplices.[20] After reviewing the cell phone records of the accomplices, the FBI identified Carpenter and several additional individuals that the accomplices had called during the robberies.[21] Subsequently, the FBI applied for and were granted three court orders under the Stored Communications Act ("SCA")[22] that compelled Carpenter's wireless carriers—MetroPCS and Sprint—to disclose cell-site location information ("CSLI"), including 152 days of CSLI data from MetroPCS and seven days from Sprint.[23] Since the FBI obtained the CSLI under the SCA, a warrant was not required.[24] Using the cell-site information collected by Sprint and MetroPCS, the FBI concluded that Carpenter

14. 442 U.S. 735 (1979).

15. *See infra* Part IV.A

16. *See infra* Part IV.B.

17. *Carpenter*, 138 S. Ct. at 2221.

18. *See Id.*; *see also infra* Part IV.C.

19. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

20. *Id.*

21. *Id.*

22. The Stored Communication Act permits the government to obtain certain telecommunications records when "specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. 18 U.S.C. § 2703(d).

23. *Carpenter*, 138 S. Ct. at 2212. CSLI is "a time-stamped record" that is generated when cellphones connect to cell-sites. *Id.* at 2211. The Court noted that "[w]ireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. . . . Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI." *Id.*

24. *Id.* at 2212.

was near four of the robberies at the time they occurred.[25] Carpenter was charged with six counts of robbery and six counts of carrying a firearm.[26]

Before trial, Carpenter moved to suppress the CSLI record that the FBI obtained from Carpenter's wireless carrier without a warrant.[27] He argued that the warrantless seizure of the CSLI records violated his Fourth Amendment rights.[28] After the district court denied Carpenter's motion, Carpenter was convicted of all counts but one firearm charge.[29] The Sixth Circuit affirmed Carpenter's conviction based on the third-party doctrine and held that Carpenter had no reasonable expectation of privacy in the cell-site location data because he voluntarily shared that information with his wireless carriers as "a means of establishing communication[.]"[30] The Sixth Circuit reasoned that the CSLI records are considered business records that are not afforded Fourth Amendment protections.[31]

Judge Stranch wrote a concurring opinion in which he addressed the Fourth Amendment concerns over "the sheer quantity of sensitive information procured without a warrant in this case" and "the nature of the tests we apply in this rapidly changing area of technology[.]"[32] Most notably, Judge Stranch pointed out that the third-party doctrine "is ill suited" to the digital age where technology advances allows for more intrusive, personal surveillance.[33] In light of the intrusive, personal data being collected, precedent signifies the need for a new test to determine when a warrant is required. [34] The Supreme Court granted certiorari.[35]

II. Legal Background

To understand the Court's shift in Fourth Amendment jurisprudence in *Carpenter*, it is important to discuss the constitutional protections of the Fourth

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.* at 2212-13. Carpenter was sentenced to over 100 years in prison. *Id.* at 2213.

30. United States v. Carpenter, 819 F.3d 880, 888, 890 (6th Cir. 2016) (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979)).

31. *Id.* at 890.

32. *Id.* at 893-94 (Stranch, J., concurring).

33. *Id.* at 894 (Stranch, J., concurring). Judge Stanch suggested that "[i]n light of the personal tracking concerns articulated in our precedent, [he was] not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location." *Id.* at 895. He goes further to express his concerns with the applicability of the third-party doctrine due to its limitless ability to collect long and extensive records. *Id.*

34. *Id.* at 894-96 (Stranch, J., concurring).

35. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

Amendment[36] and how the Fourth Amendment applies in a non-digital world[37] compared to a digital one.[38]

A. Fourth Amendment Jurisprudence

The Fourth Amendment states "[t]he 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[.]"[39] By including "in their persons, houses, papers, and effects" within the Fourth Amendment, the framers foreshadowed the importance of the Amendment's close connection to property in Fourth Amendment jurisprudence.[40] Historically, when determining whether the government's intrusion constituted a search, the Court examined whether the government "obtain[ed] [the] information by physically intruding on a constitutionally protected area."[41] Therefore, Fourth Amendment protections were only triggered when physical intrusions occurred.[42]

However, in *Katz v. United States*,[43] the Court shifted its understanding of the Fourth Amendment towards a newfound interest in protecting certain expectations of privacy as well.[44] In *Katz*, the FBI attached a listening device to a public phone booth to record the defendant's conversations.[45] In determining whether this invasion constituted a search within the meaning of the Fourth Amendment, the Court noted that "the Fourth Amendment protects people and not simply 'areas'—against unreasonable searches and seizures[.]"[46] The Court went further to explain that "the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[47] The approach used by the Majority in *Katz* — the common-law trespass approach—is no longer controlling. Instead, Justice Harlan's concurring opinion in *Katz* sets forth a new test for determining

36. *See infra* Part II.A.

37. *See infra* Part II.B.

38. *See infra* Part II.C.

39. U.S. CONST. amend. IV.

40. U.S. CONST. amend. IV. *See also* United States v. Jones**,** 565 U.S. 400, 405 (2012) (noting that "the phrase 'in their persons, houses, papers, and effects' would have been superfluous" if the Framers did not intend, at least in part, for the Fourth Amendment to be "tied to common-law trespass").

41. *Jones*, 565 U.S. at 413 (internal quotations omitted).

42. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that "the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment" because the search and seizure refers to an "actual physical invasion" of one's person, papers, tangible material effects, or home - not their conversations).

43. Katz v. United States, 389 U.S. 347, 353-58 (1967).

44. *Id.* at 353-58 (majority opinion); *Id.* at 360-61 (Harlan, J., concurring).

45. *Id.* at 348.

46. *Id.* at 353.

47. *Id.*

what constitutes a search: the reasonable expectation of privacy test.[48] This test has "a twofold requirement, first[,] that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[49]

After *Katz*, the Supreme Court has made clear that, as it stands, one has Fourth Amendment protection if either (1) law enforcement trespasses one's person, house, paper, or effect,[50] or (2) if law enforcement violates one's subjective expectation of privacy ("SEOP") which society is prepared to recognize as reasonable ("REOP").[51] Nevertheless, the Court developed an exception to these protections for when people voluntarily cede information to third parties: the third-party doctrine.[52]

B. The Development of the Third-Party Doctrine in a Non-digital World

In the 1970s, the Court decided two landmark cases where it declined to extend Fourth Amendment privacy protections[53] to information one voluntarily provides to third parties: *United States v. Miller*[54] and *Smith v. Maryland*.[55] The court reasoned that society ". . . no longer recognized the expectation of privacy involving information. . ." ceded to third parties as reasonable, it declined to extend Fourth Amendment privacy protections in such circumstances.[56]

In *Miller*, the Bureau of Alcohol, Tobacco, and Firearms ("ATF") was investigating the defendant for violating tax and firearm statutes.[57] In an effort to prove that the defendant was in possession of unpaid whiskey and alcohol equipment, the ATF issued subpoenas to the defendant's bank to compel his bank statements.[58] The

48. *Id.* at 360 (Harlan, J., concurring).

49. *Id.* at 361 (Harlan, J., concurring).

50. *See* United States v. Jones, 565 U.S. 400, 405 (2012) (noting "our Fourth Amendment jurisprudence was tied to common-law trespass").

51. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

52. *See infra* Part II.B.

53. *See supra* Part II.A.

54. 425 U. S. 435 (1976).

55. 442 U.S. 735 (1979).

56. *See Miller*, 425 U.S. at 443 (noting that "[t]his Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [a third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

57. *Id.* at 437.

58. *Id.* The defendant moved to suppress the bank statements, but the district court denied. *Id.* at 438-39. The Court of Appeals reversed and held that "the Government had improperly circumvented *Boyd's* protections of respondent's Fourth Amendment right against 'unreasonable searches and seizures' by 'first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies.'" *Id.* at 439 (quoting United States v. Miller, 500 F.2d 751, 757 (5th Cir. 1974)).

bank statements led to the defendant's conviction.[59] On appeal, the Supreme Court considered whether the seizure of the defendant's bank statements that were obtained without a warrant violated his Fourth Amendment rights.[60] The Court "examine[d] the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[61] The Court held that the defendant did not have a Fourth Amendment interest since the documents subpoenaed were business records rather being than the defendant's private papers.[62] The Court effectively created what is now known as the third-party doctrine when it noted:

that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[63]

Three years later, in *Smith v. Maryland*,[64] the Court applied the third-party doctrine to a case involving a pen register, a device that records the phone numbers dialed to a specific location.[65] In considering whether the police department's warrantless use of a pen register violated the defendant's Fourth Amendment rights,[66] the Court held that the "'installation and use of a pen register . . . was not a 'search,' and no warrant was required."[67] The Court reasoned that there was "no actual expectation of privacy in the phone numbers [the defendant] dialed, and that, even if [the defendant] did, [the defendant's] expectation was not 'legitimate.'"[68] The Court applied *Miller's* business record standard, and noted that people know, or should know, that the numbers they dial go directly to the phone company, are published in a public phonebook, and that the information is therefore voluntarily provided to third parties.[69]

59. *Id.* at 438.
60. *Id.* at 439.
61. *Id.* at 442.
62. *Id.* at 440, 444.
63. *Id.* at 443.
64. 442 U.S. 735 (1979).
65. *Id.* at 737.
66. *Id.* at 736.
67. *Id.* at 745-46.
68. *Id.* at 745.
69. *Id.* at 742-43.

C. Shifting Fourth Amendment Jurisprudence Towards Protecting Privacy Rights in the Digital Age

As technology advanced, courts began "struggling to determine if (and how)" the third-party doctrine should be applied in the digital age.[70] In *United States v. Jones*,[71] the FBI was investigating the defendant for drug trafficking when it installed a GPS device to the defendant's vehicle without a warrant and monitored him for 28 days.[72] Based on this information, the defendant was charged with and convicted of drug trafficking.[73] The Court considered whether the installation and use of the GPS tracking device on the defendant's vehicle, without a warrant, constituted a search in violation of the Fourth Amendment.[74] Noting that the defendant's "Fourth Amendment rights do not rise or fall with the *Katz* formulation[,]" the Court held that the surveillance practice constituted a search.[75] Since this holding was not based on *Katz's* analytical framework, the Fourth Amendment protections in this case are rooted in common-law trespass.[76]

The concurring justices—Justices Sotomayor and Alito—examined the pervasiveness of the governmental intrusion rather than the physical invasion of the surveillance practice.[77] Justice Alito focused on the length of time the government employed its surveillance methods.[78] In Justice Alito's opinion, Fourth Amendment protections were only warranted for longer-term monitoring.[79] Although Justice Sotomayor agreed that long-term monitoring warranted Fourth Amendment protections, she noted that "even [in] short-term monitoring," technological-advanced monitoring methods can still "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[80]

70. United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (Stranch, J., concurring).

71. 565 U.S. 400 (2012).

72. *Id.* at 402. The GPS captured more than 2,000 pages of data. *Id.* at 403.

73. *Id.* at 403-04. Specifically, the defendant was convicted of "conspiracy to distribute and possession with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base. *Id.* The defendant moved to suppress the information seized from the warrantless GPS report, but the district court denied. *Id.*

74. *Id.* at 402.

75. *Id.* at 405. "[T]he Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Id.* at 404. The Court noted that it has "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* at 404-05.

76. *Id.* at 405.

77. *Id.* at 413-15, 419 (Sotomayor, J., concurring); *Id.* at 419 (Alito, J., concurring).

78. *Id.* at 430 (Alito, J., concurring).

79. *Id.* (Alito, J., concurring) (noting that "[r]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

80. *Id.* at 415 (Sotomayor, J., concurring).

Justice Sotomayor's focus on the pervasiveness and characteristics of the surveillance methods illustrated a shift in Fourth Amendment jurisprudence towards examining the technology itself.[81] Instead of solely looking at who the information is being provided to, the Court was beginning to also examine the attributes of the surveillance practice "when considering the existence of a reasonable societal expectation of privacy."[82]

In summary, history and precedent illustrates the Court's shift towards focusing on the technology itself—its revealing nature, its collection process, and its advanced properties compared to surveillance practices in the pre-digital world—rather than to whom the information is being provided to.[83] As many government intrusions would not have been possible with previous surveillance practices, Justice Alito's and Justice Sotomayor's applications of an equilibrium-adjustment theory[84] became a central component in *Carpenter*.[85]

III. THE COURT'S REASONING

Writing for the majority in *Carpenter v. United States*,[86] Chief Justice Roberts held that "[t]he Government's acquisition of the cell-site records . . . was a search[,]"[87] and therefore, required a warrant under the Fourth Amendment.[88] The Court reasoned that "the *deeply revealing nature of CSLI*, its *depth*, *breadth*, and *comprehensive reach*, and the inescapable and *automatic nature* of its collection"[89] as seen in this case "implicates privacy concerns [that go] far beyond those considered" when the third-party doctrine was founded.[90] In declining to extend the third-party doctrine set forth in *Smith* and *Miller*,[91] the Court instead examined the unique characteristics of CSLI records and the extensive personal information it collects.[92] Unlike in the 1970's, today's technology reveals far more personal information than what the Court could imagine when it developed the third-party

81. *Id.* at 416 (Sotomayor, J., concurring). "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance." *Id.* at 415.

82. *Id.* at 416.

83. *Id.* at 413-15, 419 (Alito, J. & Sotomayor, J., concurring).

84. *See infra* Part IV.B.2.

85. *See infra* Part IV.B.

86. 138 S. Ct. 2206 (2018).

87. *Id.* at 2223.

88. *Id*. at 2221.

89. *Id.* at 2223 (emphasis added).

90. *Id.* at 2220.

91. *Id.* at 2217.

92. *Id.* at 2223 (emphasis added).

doctrine.[93] The Court further noted that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information *casually* collected by wireless carriers today."[94] In doing so, the Court held that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[95]

The Court recognized technology's advancement and noted the importance of preserving one's privacy interest against the increasing level of governmental intrusion.[96] As CSLI and new, advancing technology allow law enforcement and government officers to better understand the composition of one's personal life, society's privacy concerns are increasing.[97]

In addition to the difference in the nature of information being collected in the digital age, the Court also examined the second component of the third-party doctrine: voluntary exposure.[98] In holding that this component also does not "hold up when it comes to CSLI," the Court emphasized that cellphones "log[] a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[99] Since phone users do not truly share their information to third parties, the Court held that Fourth Amendment protections are warranted.[100] Thereby, the Court emphasizes the key role digital technology plays in the government's ability to perform new surveillance methods and collect more pervasive information.[101]

The Court further held that the Government generally must obtain a warrant prior to search CSLI records.[102] The Court reasoned that new digital technologies that record a detailed log of one's movements for an extended period of time should be granted Fourth Amendment protections, as people have a reasonable expectation of privacy in such information.[103] It noted that "CSLI is an entirely

93. *Id.* at 2220. *See generally* Kyllo v. United States, 533 U.S. 27, 29-30, 35 (2001) (holding that the government's use of an external thermal-imaging device to detect the growth of marijuana inside a home constituted a search, and any alternative outcome "would leave homeowners at the mercy of advancing technology").

94. *Id.* at 2219 (emphasis added).

95. *Id.* at 2217, 2220.

96. *Id.* at 2214. The Court seeks to ensure the protections afforded by the Fourth Amendment when it was adopted. *Id.*

97. *Id.* at 2218.

98. *Id.* at 2220.

99. *Id.* The Court prefaces this by noting that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.*

100. *Id.*

101. *Id.* at 2219.

102. *Id.* at 2221.

103. *Id.* at 2221-22.

different species of business record [that] concerns [] arbitrary government power much more directly than corporate tax or payroll ledgers."[104]

IV. ANALYSIS

In *Carpenter v. United States*,[105] the Court held that the Government violated Carpenter's Fourth Amendment rights against unreasonable searches and seizures when it used CSLI to track his past movements over the course of seven days.[106] The Court correctly declined to extend the third-party doctrine from *Miller*[107] and *Smith*[108] to CSLI.[109] In doing so, the Court properly identifies a seismic shift in digital technology, but erroneously declines to expressly adopt a new application of the third-party doctrine.[110] The Court's holding may have greater implications in future third-party cases, especially those involving disease surveillance.[111]

A. The Court Correctly Declined to Extend the Third-Party Doctrine from Miller and Smith

Writing for the Majority in *Carpenter v. United States*, Chief Justice Roberts correctly declined to extend *Miller*[112] and *Smith*[113] to CSLI, a "a time-stamped record" of one's movement generated when cellphones connect to a cell site.[114] As noted in Part III, courts examine two key components when applying the third-party doctrine: the nature of the device/surveillance practice and the voluntary exposure of the material.[115] Together, one does not have a "legitimate expectation of privacy in information he voluntarily turns over to third parties[,]"[116] even if he does so under the "assumption that it will be used only for a limited purpose[.]"[117] However, the documents sought in *Smith*[118] and *Miller*[119] were less intrusive than the CSLI at

104. *Id.* at 2222.
105. 138 S. Ct. 2206 (2018).
106. *Id.* at 2223.
107. 425 U.S. 435 (1976).
108. 442 U.S. 735 (1979).
109. *See infra* Part IV.A.
110. *See infra* Part IV.B.
111. *See infra* Part IV.C.
112. *Miller*, 425 U.S. at 435.
113. *Smith*, 442 U.S. at 735.
114. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
115. *See supra* Part II.C; s*ee also Carpenter*, 138 S. Ct. at 2219-2220 (noting that the two rationales underlying the third-party doctrine are the nature of the document and its voluntary exposure).
116. *Smith*, 442 U.S. at 743-44.
117. *Miller*, 425 U.S. at 443.
118. 442 U.S. 735 (1979).
119. 425 U. S. 435 (1976).

issue here, which has the ability to produce a comprehensive log of one's physical movements.[120]

Justice Sotomayor's concurrence in *Jones* helped shape the Court's reluctance to extend the third-party doctrine in this case. Justice Sotomayor noted that some new technology creates a "precise, comprehensive record . . . about [one's] familial, political, professional, religious, and sexual associations."[121] Like the GPS tracking device at issue in *Jones*, CSLI can also reveal a complete record of one's locations for an extended period.[122] CSLI technology goes even further to eliminate the voluntary exposure component of the third-party doctrine, because the record is created "by dint of its operation, without any affirmative act on the part of the user beyond powering up."[123]

The third-party doctrine was created as an exception to the Fourth Amendment's warrant requirement.[124] This exception was limited to business-like records that were voluntarily provided to third parties.[125] Given that CSLI information (1) no longer requires a user to affirmatively assent to cede third parties with information[126] and (2) is more comprehensive and pervasive than any business-like records at issue in *Smith*[127] and *Miller*,[128] the principles of the third-party doctrine cannot be upheld.[129] If the Court had applied the third-party doctrine in *Carpenter*, the Founders' intent for enacting this Amendment would not have been upheld.[130]

120. *Carpenter,* 138 S. Ct. at 2219-20.

121. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

122. *Carpenter,* 138 S. Ct. at 2220.

123. *Id.* The Court also notes that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society", thus making the information provided under the use of CSLI technology in this manner involuntary. *Id.*

124. *Miller*, 425 U. S. at 443.

125. *Id.*

126. *Carpenter,* 138 S. Ct. at 2220.

127. 442 U.S. 735 (1979).

128. 425 U.S. 435 (1976).

129. *Carpenter,* 138 S. Ct. at 2220.

130. See Brain Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/blog/privacy-technology/location-tracking/what-founders-would-say-about-cellphone-surveillance (arguing that a government's use of CSLI to track the whereabouts of its users is "disconcerting" and is "contrary to the text and original meaning of the Fourth Amendment" as the "Founders recognized that giving the state arbitrary search power harms "the people" in ways that go beyond the indignity of specific trespasses").

B. The Court Correctly Identifies the Seismic Shift in Digital Technology, but Incorrectly Declines to Reconstruct the Third-Party Doctrine.

In declining to extend *Miller*[131] and *Smith*,[132] the Court correctly identifies how advances in technology require a narrower application of the third-party doctrine.[133] As the third-party doctrine is an exception to the *Katz* understanding of one's reasonable expectation of privacy, the Court identifies the need to now focus "on how much the government can learn about a person regardless of the place or thing from which the information came [from]."[134] When technology facilitates a "too permeating police surveillance[,]" Fourth Amendment protections are likely triggered.[135] Courts have "struggl[ed] to determine if (and how) existing tests apply or whether new tests should be framed" when dealing with new technology. [136] Given that the Court now focuses on the mechanics of the surveillance practice in the digital age—what, how, and for how long is information being collected— the Court erroneously fails to reconstruct the third-party doctrine to accommodate these advancements in future cases.

a. A Systematic Shift in Fourth Amendment Jurisprudence

The Fourth Amendment was adopted nearly 90 years prior to the invention of a major factor in *Carpenter*: the cellphone.[137] Consider a 2018 study by Douglas C. Schmidt, a professor at Vanderbilt University, outlining Google's data collection approaches.[138] This study indicates that of the 900+ information requests Google makes to Android phones per day, nearly 35% of them are for location

131. *Miller*, 425 U.S. at 435.

132. 442 U.S. 735 (1979).

133. *Carpenter*, 138 S. Ct. at 2220; *see also* MICHAEL A. FOSTER, CONG. RSCH. SERV.: LEGAL SIDEBAR, LSB10449, COVID-19, DIGITAL SURVEILLANCE, AND PRIVACY: FOURTH AMENDMENT CONSIDERATIONS (2020*)* (noting that the Court in *Carpenter* "appeared to retreat from a broad conception of the third-party doctrine, at least as applied to certain kinds of digital information held by third-party companies").

134. Orin S. Kerr, *Implementing Carpenter*, THE DIGIT. FOURTH AMENDMENT (forthcoming) (manuscript at 6), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257.

135. *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re*,* 332 U.S. 581, 595 (1948)).

136. United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (Stranch, J., concurring).

137. Judge Herbert B. Dixon, Jr., *Telephone Technology versus the Fourth Amendment*, AM. BAR ASS'N (May 1, 2016), https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/.

138. Douglas C. Schmidt, *Google Data Collection*, DIGIT. CONTENT NEXT (Aug. 15, 2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf. "The most obvious are 'active,' with the user directly and consciously communicating information to Google, as for example by signing in to any of its widely used applications such as YouTube, Gmail, Search etc. Less obvious ways for Google to collect data are 'passive' means, whereby an application is instrumented to gather information while it's running, possibly without the user's knowledge." *Id.*

information.[139] Realizing a similar attribute to CSLI, the Court noted that "the unique nature of cell phone location records" limits the application of the third-party doctrine.[140] The Court further observed that the digital age allows the Government to intrude on one's privacy in a way that would have been protected by the Fourth Amendment prior to the digital age.[141] Scholars also articulate that modern-day society has an increased expectation of privacy in digital technology, such as cellphones, that warrants protections against a greater level of governmental intrusion.[142]

Prior to the digital world, the Supreme Court held that a search was limited to merely physical intrusions.[143] However, as time progressed, this definition shifted from protecting places to protecting people.[144] Although this protection was later limited depending on what information was provided[145] and to whom,[146] the Court began to broaden its application of Fourth Amendment protections as new technology emerged.[147]

By shifting towards a focus on whether the "technology changed [one's] expectations of what the police *can do*" rather than on who the information was provided to,[148] Fourth Amendment protections will likely be adjusted to conform to these "near perfect surveillance" methods.[149] Consequently, the *Carpenter* Court identified the significance of advancing technology on government intrusions, and

139. *Id.*

140. *Carpenter*, 138 S. Ct. at 2220.

141. *Id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)). The court noted that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Id.* The Court further noted that "[p]rior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.' For that reason, 'society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.'" *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring)).

142. Daniel K. Gelb, *Why Carpenter v. United States Warrants a Warrant for Our Whereabouts*, PROQUEST, Spring 2018, at 35, 36.

143. Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that a wiretap "did not amount to a search or seizure within the meaning of the Fourth Amendment," because there was no "official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house").

144. Katz v. United States, 389 U.S. 347, 353 (1967).

145. *Id.* at 352 (noting that the audio of the surveillance is content); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (noting that the information in an email is content).

146. United States v. Miller, 425 U.S. 435, 443 (1976).

147. *See supra* Part II.C.

148. Kerr, *supra* note 135.

149. Carpenter v. United States, 138 S. Ct. at 2206, 2218 (2018).

implicitly applied an equilibrium adjustment theory to the CSLI technology in this case.

b. The Equilibrium-Adjustment Theory

The Court has shifted its application of the third-party doctrine to restore the protections under the Fourth Amendment.[150] This application is known as the Equilibrium-Adjustment theory—a theory "posit[ing] that the Supreme Court [should] adjust[] the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection."[151] In other words, "when changing technology or social practice expands government power, the Supreme Court tightens Fourth Amendment protection; when it threatens government power, the Supreme Court loosens constitutional protection."[152]

As technology advances, courts have revisited the level of intrusion the new technology or surveillance practice entails. For example, thirty years after *Smith* was decided, the Court in *United States v. Jones* considered whether attaching a GPS tracking device on a person's vehicle without a warrant to monitor its movements for an extended period of time violated the Fourth Amendment.[153] Although the majority held that this level of intrusion violated the Fourth Amendment on trespassing grounds,[154] Justice Sotomayor and Alito are most noteworthy in foreshadowing the reasoning in *Carpenter*.[155] As mentioned above,[156] Justice Sotomayor's opinion focused on the pervasiveness of a GPS monitoring device[157] and stated that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[158] Justice Alito also focused on the pervasiveness of the technology, but instead of relying on the intrusion into one's identity, focused on the length of time the GPS tracking device was used.[159]

150. *See supra* Part II.B, II.C.

151. Kerr, *supra* note 135.

152. *Id.*

153. 565 U.S. 400, 402 (2012).

154. *Id.* at 404-05.

155. *Id.* at 417 (Sotomayor, J., concurring) (noting that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

156. *See* Part II.C.

157. *Id*. at 416 (Sotomayor, J., concurring) (noting that she "would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy . . . in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

158. *Id.* at 415.

159. *Id.* at 430 (Alito, J., concurring); *see also supra* Part II.C.

Modern-day technology has unique characteristics that were not available when the Fourth Amendment was adopted.[160] Accordingly, the Court has indirectly applied an equilibrium-adjustment approach to match the advancing technology of CSLI.[161] Since precedent illustrates a court's willingness and eagerness to adjust for the digital age in order to protect consumers' information,[162] they provide to third parties, the Court should reconstruct the third-party doctrine to provide uniformity amongst the courts. The Court could reconstruct the doctrine to become more of a balancing test where courts should balance the (1) revealing nature, depth, and breadth of the information being obtained; (2) who is collecting the information; (3) how users are exposing themselves to the seizure; and (4) how capability of the technology itself differs from common-law trespass. Given most modern technologies are becoming a "pervasive and insistent part of daily life," the third-party doctrine is inevitably going to become limited in scope, and therefore, needs to be modernized.[163]

C. Post-Carpenter Implications on Disease Surveillance

Although *Carpenter* did not address short-term CSLI tracking nor the use of other traditional surveillance techniques and tools,[164] the fact that who information is provided to is now merely a factor in assessing one's reasonable expectation of privacy is likely to heighten Fourth Amendment protections. This is especially true as governments begin to surveil individuals to combat the spread of COVID-19—the disease caused by the novel coronavirus Sars-Cov-2.[165] For example, technology companies and some state governments began tracking cellphone users' location data to create a log of individuals who may have come in contact with an infected person.[166] With this endeavor creating "a host of legal issues[,]" courts will need to determine how *Carpenter* should be applied in disease surveillance.[167]

Even though *Carpenter* was limited solely to CSLI, the Constitution's Framers intended the principles of the Fourth Amendment to apply to "all forms of privacy invasion[s]."[168] If the government and private companies decided to use mass

160. *See* Dixon, *supra* note 138.

161. *See* Evan Caminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 418-23 (2018); *see also Jones*, 565 U.S. at 415).

162. *See supra* Part II.B.

163. Riley v. California, 573 U.S. at 373, 385 (2014).

164. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

165. *See* FOSTER, *supra* note 134.

166. *Id.*

167. *Id.*

168. Albert f. Cahn & Zachary Silver, *Is COVID-19 Deadly to the Fourth Amendment?*, SURVEILLANCE TECH OVERSIGHT PROJECT (July 15, 2020), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5f15c8647370541bfad430e9/1595263077585/2020-05-27%2BIs%2BCOVID%2BDeadly%2Bto%2Bthe%2BFourth%2BAmendment.pdf.

surveillance to track the spread of COVID-19, they will need to overcome the following requirements applied in *Carpenter* for the surveillance method to fall outside the scope of the third-party doctrine: (1) the "collection of information [must be] made widely possible by surveillance methods of the digital age[;]" (2) the "records must not be the product of a user's meaningful voluntary choice[;]" and (3) "the records must be of a type that tends to reveal an intimate portrait of a person's life beyond the legitimate interests of criminal investigations . . . such as [one's] personal associations, religious beliefs, sexual preferences, and political views."[169]

a. Category One: The Information Collected Must be Made Possible by Surveillance Methods of the Digital Age

Many tech companies are using cellphone geolocations to track the spread of COVID-19.[170] Their ability to even track COVID-19 using this type of surveillance method is only made possible due to our ability to carry our cellphones wherever we go.[171] If, however, the government tries to use traditional surveillance devices such as security cameras to monitor the spread of the virus and compliance with stay-at-home orders, Fourth Amendment protections are unlikely to be triggered, as these devices may not present the same comprehensive log of one's intimate details of his movements.[172] Therefore, the first question in the use of disease surveillance would be what type of device or surveillance practice is being used. The more comprehensive and intrusive means of surveillance will have a greater likelihood of being held unconstitutional, as it is more likely to be protected by the Fourth Amendment.

b. Category Two: Voluntary Exposure

For disease surveillance, the voluntary exposure concerns laid out in *Carpenter* are likely to be invoked. Like the automatic nature of CSLI's collection process, several tech companies are incorporating an automatic enrollment to the government's COVID-19 tracking through the mere action of using a particular app.[173] Additionally, several phone users have reported a continuous popup

169. Kerr, *supra* note 135, at 3.

170. *See* FOSTER, *supra* note 134.

171. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

172. *Id.* at 2220. In *Carpenter*, the Court noted that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.*

173. *See* FOSTER, *supra* note 134 (noting that Google and Facebook have discussed using their location data voluntarily provided by to track its' users movement during the pandemic).

notification to enroll in said program.[174] As many establishments are implementing COVID-19 restrictions, users may believe that they are required to enroll.[175] In turn, this effectively diminishes the voluntariness of a user's consent to provide third parties with their personal movements and should likely make this form of surveillance unconstitutional.

c. Category Three: The Revealing Nature of the Information Collected

Although the intent of this disease surveillance is to combat the spread of COVID-19, law enforcement may try to compel user records from the tech companies. Like the CSLI technology in *Carpenter*, disease surveillance may also "provide[] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[176] If individuals opt into this surveillance practice, the question seemingly turns to how long the government intruded.[177] For instance, say one begins using a phone application that partakes in this disease surveillance. If the government begins tracking him on day one and can link him to a particular crime by day four, will this intrusion fall outside the scope of *Carpenter*? Under a textual lens, this type of instruction would because *Carpenter* did not address surveillance methods, even those of similar comprehensive and pervasive magnitudes, that involved fewer than seven days of intrusion.[178] However, given that one could argue that all three requirements are satisfied to obtain Fourth Amendment protections, courts will likely hold that this type of surveillance practice falls outside the typical REOP standard for third-party doctrine cases.

Nevertheless, courts may be able to limit the implications of declining to extend the third-party doctrine in said cases if the government invokes the special needs warrant exception. This exception authorizes warrantless searches when "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable."[179] Thereby, warrantless searches in these circumstances would be made reasonable.[180] Although COVID-19 may provide grounds for a mass data collection, the intent for the surveillance may not be one that creates a "special need" that makes obtaining a "warrant and probable

174. Reed Albergotti, *Apple and Google Expand Coronavirus Warning Software*, THE WASH. POST (Sept. 1, 2020), https://www.washingtonpost.com/technology/2020/09/01/apple-google-exposure-notification-express/.

175. *Id.*

176. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 566 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

177. *See* FOSTER, *supra* note 134.

178. *Carpenter*, 138 S. Ct. at 2220, n.3.

179. New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

180. *Id.*

cause impracticable."[181] Instead, the public health emergency authorizes the use of the data collection for the said purpose of combating the spread of the virus, not to combat criminal behavior during the pandemic.[182] There is no linkage between a special need to curtail the warrant requirement in criminal investigation with the need to combat the spread of COVID-19.

Although the special needs doctrine has not been evaluated in third-party doctrine cases,[183] the special needs warrant requirement is unlikely to apply in these circumstances. The pervasiveness of the disease surveillance, like the pervasiveness of the CSLI in *Carpenter*,[184] would likely require law enforcement to obtain a search warrant prior to obtaining record from third parties.

CONCLUSION

In *Carpenter v. United States*,[185] the Supreme Court held that the use of cell-site location information constituted a Fourth Amendment search, requiring a warrant due to the pervasiveness of the technology.[186] The Court correctly declined to extend the third-party doctrine set forth in *Miller*[187] and *Smith*[188] to CSLI data capture.[189] As a result, the Court correctly identifies a seismic shift in digital technology, but erroneously fails to expressly modernize the third-party doctrine for the digital age.[190] The Court's decision has potential to create murky territory surrounding disease surveillance in the age of COVID-19, as it may cause confusion amongst the courts on how to balance governmental interests against privacy interests when surveilling the spread of COVID-19. [191]

181. *Id.*

182. *See* FOSTER, *supra* note 134.

183. *See* Cahn & Silver, *supra* note 163.

184. Carpenter v. United States, 138 S. Ct. 2206, 2217-20 (2018).

185. *Id.* at 2206.

186. *Id.* at 2223. The Court relied on the "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection" in coming to their holding. *Id.*

187. 425 U. S. 435 (1976).

188. 442 U.S. 735 (1979).

189. *See supra* Part IV.A.

190. *See supra* Part IV.B.

191. *See supra* Part IV.C.

SHELBY MCCLOSKEY

Carpenter v. United States