Florida Law Review

Volume 72 | Issue 4 Article 5

July 2020

Implications of the Third-Party Doctrine: The New Age of Digital Data and Carpenter

Chelsea Ann Padgett

IMPLICATIONS OF THE THIRD-PARTY DOCTRINE: THE NEW AGE OF DIGITAL DATA AND *CARPENTER*

Chelsea Ann Padgett[*]

Abstract

This Note addresses cell-site location information and the third-party doctrine while deeply analyzing the U.S. Supreme Court's recent decision in *Carpenter v. United States*. This case has proven itself quite uninformative as it left the third-party doctrine in a state of disarray and confusion. This Note argues that there is no Fourth Amendment protection for information held and developed by a third-party cell phone carrier, even with technological advances such as cell-site location information. Because the information is produced by an individual's cell phone carrier stamping the individual's phone with the location of the cell tower from which it is pulling its service, the user has effectively consented to such information being shared with a third party and is at least somewhat aware that the cell-site location information, along with the phone number dialed, can be provided to the police without a warrant. There are effective measures, both legislative and judicial, that if implemented will help fix these privacy issues arising out of technological advances.

* J.D., University of Florida Levin College of Law 2020; B.A., University of North Florida 2017. I dedicate this Note to my parents, Ted and Michelle Padgett, who have always supported my goals, and to all my friends who have encouraged me along the way. I would also like to thank Professor Stinneford for his guidance throughout the note-writing process and Professor Priester for sparking my interest in criminal procedure.

INTRODUCTION

When the U.S. Supreme Court grants certiorari in a case, it is assumed that, regardless of the outcome, the American people will have a better understanding of the law by which they must abide. However, when the Court releases a narrow opinion that fails to answer significant questions, it leaves individuals confused and concerned about what the law truly is. This is exactly what has happened since the recent decision of *Carpenter v. United States*[1]—a case that rattled the effects of the third-party doctrine with regard to digital data. In *Carpenter*, the Court addressed a single issue: whether access to historical cell phone records providing a comprehensive chronicle of the user's past movements constitutes a search deserving protection under the Fourth Amendment.[2] This issue is extremely pertinent to the new age of smartphones and digital data; however, the Court left behind too many unanswered questions. With these questions left unanswered, the opinion fails to explain what it means for the third-party doctrine as a whole. In a 5–4 decision, the Court determined that access to a user's past movements through a cell phone carrier is much the same as the Global Positioning System (GPS) tracking in *United States v. Jones*.[3] However, the Court stated that this opinion does not affect the well-known third-party doctrine cases—*United States v. Miller*[4] and *Smith v. Maryland*.[5]

Considering that the third-party doctrine itself is a derivative of such cases, it is difficult to understand why the *Carpenter* Court would hold that cell phone records held by a third party are more analogous to *Jones*. This case should not have been decided based on how "effortlessly" such cell phone data can be compiled[6] or how such information resembles that of the GPS[7] but instead on how and under what circumstances that information is retrieved. The Court stated that a time-stamped record

1. 138 S. Ct. 2206 (2018).

2. *Id.* at 2211.

3. 565 U.S. 400, 404 (2012) (deciding that the government's installation of a GPS device on a target's vehicle and its use of that device to monitor the vehicle's movements constitute a physical "search" of private property); *see Carpenter*, 138 S. Ct. at 2217.

4. 425 U.S. 435 (1976).

5. 442 U.S. 735 (1979); *see Carpenter*, 138 S. Ct. at 2217.

6. *Carpenter*, 138 S. Ct. at 2216.

7. *See GPS: The Global Positioning System*, GPS.GOV, https://www.gps.gov [https://perma.cc/C82U-K8NB] (last updated Jan. 15, 2020) (describing GPS as a global public service of the federal government).

known as cell-site location information (CSLI)[8] is similar to that of the GPS.[9] However, this is not the case. The cell phone connects to the closest cell tower, which in return places its time-stamped CSLI record on the phone.[10] A time stamp therefore shows the relative area the user was in and in no way provides a precise location.[11]

Further, it is not out of the ordinary for someone to expect that information, such as telephone numbers dialed[12] and text messages sent,[13] is held by a third party—the phone carrier—and can be shared at any moment with the police. If a reasonable fact finder can determine that an individual's phone call and text message logs can be searched and seized without a warrant, then why is it not possible to assume that the same goes for the relative location in which the phone call or text message was made? Additionally, in the new age of digital data, smartphones are now equipped with applications (apps) such as Snapchat, Instagram, Facebook, Uber, Find My Friends, and Find My iPhone—all of which contain maps, location services, and tracking.[14] These apps, telephone calls, text messages, and location devices all have two things in common: consent and knowledge. Individuals who purchase and use cell phones have a general understanding that their telephone calls and text messages will not go through without service or Wi-Fi. Such service is provided by cell phone towers placed in a variety of locations by their cell phone provider.[15] Individuals who consent to having and using a cell phone are aware that the location in which they make a phone call is dependent on which cell phone towers are located nearby.[16] Holding that the time stamps of the cell phone towers are anything other than a means of providing effective service undermines the validity of *Smith*, *Miller*, and the entire third-party doctrine.

---

8. Cell-site location information is the data that a cell phone automatically generates each time it connects to a cell site or a cell phone tower. *See Carpenter*, 138 S. Ct. at 2211.

9. *Id.* at 2216.

10. *Id.* at 2211.

11. *See id.* at 2218.

12. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

13. *See Carpenter*, 138 S. Ct. at 2212; Callie Haslag, Note, *Technology or Privacy: Should You Really Have to Choose Only One?*, 83 MO. L. REV. 1027, 1037 (2018).

14. *See App Store*, APPLE, https://www.apple.com/ios/app-store/ [https://perma.cc/F565-K2F4]; FACEBOOK, https://www.facebook.com [https://perma.cc/8TWN-2WRH]; INSTAGRAM, https://www.instagram.com/ [https://perma.cc/E2FU-CT3W]; SNAPCHAT, https://www.snapchat.com [https://perma.cc/7EWX-D944]; UBER, https://www.uber.com [https://perma.cc/8XRN-ZTHH].

15. *See Carpenter*, 138 S. Ct. at 2211.

16. A mobile device emits electromagnetic radio waves when it tries to make a phone call, which the closest cell phone tower picks up and connects that signal to a switching center. This switching center allows the phone call to be connected to another mobile device. *See What Is a Cell Tower?*, WHAT'S A G?, https://whatsag.com/g/what-is-a-cell-tower.php [https://perma.cc/JP77-X3MQ].

In Part I, this Note discusses important background information of the search and seizure of a person's property, including the Fourth Amendment itself and important Supreme Court cases relating to the third-party doctrine. Part II analyzes the Supreme Court's ruling in *Carpenter* and why the Court granted certiorari in the case. Additionally, Part II discusses how the Supreme Court deferred important decisions within the opinion and failed to provide guidance for the third-party doctrine moving forward. In Part III, this Note addresses the implications of the *Carpenter* decision. Part III discusses three different ways in which the law can move forward from this decision to determine what exactly the third-party doctrine is in this new age. Further, Part III discusses a possible solution to the unanswered questions the Court left behind by considering how relevant aspects, such as consent and knowledge, relate to the new age of digital data. Part III also argues that the Court should have determined that the CSLI is an implied necessity to provide signal to cell phone users, which is used to make phone calls and send text messages. Because the information gathered does not amount to that of the GPS, the Court should have determined that a warrant is not required to search and seize such information if properly requested under an order from the Stored Communications Act.[17]

I. BACKGROUND

Before diving into a dense procedural analysis of the third-party doctrine, it is necessary to first understand where this doctrine came from and how it developed over time. This section will discuss the Fourth Amendment with regard to the search and seizure of a person's property. More specifically, it will discuss how the third-party doctrine has evolved throughout prominent Supreme Court cases such as *United States v. Miller* and *Smith v. Maryland*. Understanding how the third-party doctrine originated and developed is essential to properly analyze the *Carpenter* opinion and recognize its erroneous flaws.

17. Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2018)); *see* 18 U.S.C. § 2703(d) (requiring reasonable grounds for believing records are relevant to material in an ongoing investigation).

A. *A Brief Understanding of the Fourth Amendment*

The Fourth Amendment was ratified in 1791 as a part of the Bill of Rights to protect the fundamental "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[18] Further, it provides that "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."[19] However, there are several exigent circumstances that allow for a search or seizure without a warrant, including: (1) emergency aid, (2) hot pursuit, and (3) prevention of imminent destruction of evidence.[20] Up until the 1960s, the Court viewed Fourth Amendment search violations as a form of trespass upon one's property.[21] In abandoning the old trespass test, the Court determined that the two-pronged test that emerged from *Katz v. United States*[22] was better suited for analyzing Fourth Amendment search violations.[23] Justice Marshall Harlan in his concurring opinion famously introduced such test, which requires (1) "that a person have . . . an actual (subjective) expectation of privacy" and (2) that such expectation is reasonable.[24]

Although *Katz* provided an important step in the understanding of the Fourth Amendment, the ruling in *Jones* provided an alternative test—known today as governing Fourth Amendment protection.[25] *Jones* determined that the government cannot physically intrude upon persons, houses, papers, or effects to obtain information without violating the Fourth Amendment.[26] As the law has developed and become more complex over time, so has the understanding of the Fourth Amendment. For example, in 2001, the Court had to determine whether thermal-imaging devices aimed at private homes to scan for heat waves

18. U.S. CONST. amend. IV; *see* KATHLEEN M. SULLIVAN & NOAH FELDMAN, CONSTITUTIONAL LAW lxvii (19th ed. 2016).

19. U.S. CONST. amend. IV.

20. Kentucky v. King, 563 U.S. 452, 460 (2011).

21. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 67.

22. 389 U.S. 347 (1967).

23. Kerr, *supra* note 21, at 67–68.

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

25. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

26. *See id.* ("The Government physically occupied private property for the purpose of obtaining information. We have 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 406 ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))); *id.* at 411 n.8.

constituted a search within the meaning of the Fourth Amendment.[27] The Court determined that since the device was not for general public use, it was an intrusion upon an individual's person and house that would not otherwise be known without a physical intrusion, which constituted an unlawful search.[28] Further, the Fourth Amendment expanded to protect cell phone data from inherently unreasonable searches without a warrant because they contain private information that the Founders intended to protect.[29] Thus, as time progresses and new digital data devices emerge, the line between what is protected under the Fourth Amendment and what is not becomes quite blurry. The Court will look to the Fourth Amendment and established doctrinal tests to determine if such new technology fits into a category of "persons, houses, papers, and effects."[30]

B. *A Brief History of the Third-Party Doctrine*

When Fourth Amendment rights become more complicated in the face of technological advances, the Court will often turn to the third-party doctrine to maintain neutrality in applying the rules regarding such data.[31] This doctrine was created as a means for police officers to obtain information that an individual conveyed to a third party without obtaining a warrant.[32] Upon conveying that information to a third party, such as a bank[33] or a telephone carrier,[34] an individual has effectively given up any reasonable expectation of privacy in the property because the information is no longer considered private.[35] Because such information is no longer considered private, any search and seizure of the property cannot be considered a Fourth Amendment search subject to the warrant requirement.[36] The following cases set the standard for the doctrine and explain its role and effect on the Fourth Amendment.

1. *United States v. Miller*

In *Miller*, the Court held that there is no expectation of privacy in financial records held by a bank.[37] In this case, the respondent, Miller,

27. *Kyllo*, 533 U.S. at 29.

28. *Id.* at 40.

29. *See* Riley v. California, 573 U.S. 373, 386 (2014).

30. U.S. CONST. amend. IV.

31. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009).

32. *See* Simon Stern, *The Third-Party Doctrine and the Third Person*, 16 NEW CRIM. L. REV. 364, 365 (2013).

33. *See, e.g.*, United States v. Miller, 425 U.S. 435, 436–37 (1976).

34. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743 (1979).

35. *See* Stern, *supra* note 32, at 365.

36. *Id.*

37. *Miller*, 425 U.S. at 437.

moved to suppress copies of checks and bank records that police officers had obtained through court-ordered subpoenas.[38] Miller had accounts set up at two different banks but was not aware of any subpoenas.[39] The subpoenas ordered employees to make "all records of accounts, i.e., savings, checking, loan or otherwise, in the name of Mr. Mitch Miller" available for the desired agents.[40] Subsequently, the agents obtained "all checks, deposit slips, two financial statements, and three monthly statements" from one bank and were "provided with copies of one deposit slip and one or two checks" from the other.[41] Such evidence was used in Miller's trial and led to his ultimate conviction, which he appealed by claiming a violation of his Fourth Amendment rights.[42] On appeal, the court determined that the subpoenas issued were not a part of the "adequate 'legal process'" necessary for receiving such documents.[43] The government argued that the appellate court erred because (1) Miller did not have Fourth Amendment interests in the records; (2) the subpoenas were not defective; and (3) the evidence should not have been suppressed.[44] Because the Supreme Court reversed the appellate court's opinion by determining that Miller had no Fourth Amendment interest to be protected, it did not discuss arguments two and three.[45]

The *Carpenter* Court stated that this reasoning rested on two significant factors: (1) the act of sharing and (2) "the nature of the particular documents sought."[46] Because individuals are effectively "sharing" their information with a third party, it is reasonable to assume that they no longer have an expectation of privacy held within it.[47] Banks, such as in *Miller*, represent a perfect third party considering that a person deposits money and information with the expectation that it will be properly handled and cared for. Because of the need for banks in modern society, the Court explained that they are essential parties that have a substantial stake in all of the respondent's records and available funds.[48] The bank has to have control over the information given to it to function. Therefore, checks that individuals write are "not confidential

38. *Id.* at 436.

39. *See id.* at 437–38.

40. *Id.* at 437 (emphasis omitted).

41. *Id.* at 438.

42. *See id.* at 438–39.

43. *Id.* at 439 (quoting United States v. Miller, 500 F.2d 751, 758 (5th Cir. 1974), *rev'd*, 425 U.S. 435 (1976)).

44. *Id.*

45. *Id.* at 440.

46. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (quoting *Miller*, 425 U.S. at 442).

47. *Id.*

48. *See Miller*, 425 U.S. at 440.

communications but negotiable instruments to be used in commercial transactions."[49] Thus, an individual takes the risk of his documents being revealed to the government and used in an ordinary course of business by revealing such information to a third party, such as a bank.[50] Due to this lack of privacy, the Court determined that the documents obtained by the government were not "private papers" but instead "business records" that an individual cannot assert ownership or possession over.[51]

Additionally, the Court cited to the Bank Secrecy Act[52] to further its conclusion that individuals have no reasonable expectation of privacy in such records.[53] Congress passed this Act to ensure that insured depository institutions maintain adequate records because they can be useful with regard to national security and protection against domestic and international terrorism.[54] The Court prefers that information held by a third party that could prove criminal activity be accessible by law enforcement.[55] The Court assumed that such connection was relevant or else Congress would have never passed the Act in the first place.[56]

The Court concluded that all of Miller's bank documents obtained, including financial statements and deposit slips, were voluntarily conveyed to the third-party bank and lacked all reasonable expectation of privacy.[57] The physical and voluntary transfer of possession of the documents led the Court to believe that Miller relinquished his privacy rights in the property.[58] Therefore, in cases where there is no Fourth Amendment protection, a court is permitted to enter into evidence records that were obtained from a third party through issuance of a subpoena.[59] This is true even in light of a contemplated criminal proceeding.[60]

---

49. *Id.* at 442.

50. *See id.* at 442–43.

51. *Id.* at 440 (quoting Boyd v. United States, 116 U.S. 616, 622 (1886)).

52. Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 12, 15, and 31 U.S.C.).

53. *Miller*, 425 U.S. at 442–43; *see also* 12 U.S.C. § 1829b(d) (1970) (stating an express requirement to keep records of each "check, draft, or other similar instrument received" for deposit along with identification of the party's account in which the deposit is made).

54. 12 U.S.C. § 1829b(a).

55. *See Miller*, 425 U.S. at 444.

56. *See id.* at 442–43.

57. *See id.* at 443–44.

58. *See id.* at 442–43.

59. *See id.* at 444.

60. *Id.*

2. *Smith v. Maryland*

Three years after *Miller*, the Court determined that the installation and use of a pen register does not constitute a Fourth Amendment search.[61] The Court concluded that individuals do not have a reasonable expectation of privacy in dialed phone numbers and therefore the use of pen registers cannot constitute a search.[62] In *Smith*, after finding out the license plate of a man continuously making threatening phone calls to a woman whom he previously robbed, the police requested that a pen register[63] be installed on his home telephone to record any dialed numbers.[64] The police successfully traced the telephone calls received by the woman to the man's home telephone and subsequently arrested him for the robbery.[65] The Court turned to the holding in *Katz* to determine if the government obtaining the pen register information from the telephone company constituted a "search" under the Fourth Amendment.[66] A two-pronged test emerged from *Katz* that determines whether an activity constitutes a search under the Fourth Amendment: (1) whether the individual has exhibited an actual and subjective expectation of privacy and (2) whether such subjective expectation of privacy is reasonable and one that society is prepared to recognize as reasonable.[67]

The Court determined that it was doubtful that individuals hold any actual expectation of privacy in the numbers they dial on their phone because the conveyance of a phone number to the telephone company to complete a call is inevitable.[68] Further, the Court found that even if an individual has some subjective expectation of privacy in dialed phone numbers, it is not one that society is prepared to recognize as reasonable because a third party is necessary to even make phone calls.[69] Therefore, because the Court concluded that there is no reasonable expectation of privacy in telephone records voluntarily given to a third party, the *Katz* test was not satisfied.[70]

---

61. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

62. *Id.*

63. A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3) (2018).

64. *Smith*, 442 U.S. at 737.

65. *Id.*

66. *See id.* at 739.

67. *See id.* at 739–40; Katz v. United States, 389 U.S. 347, 351 (1967) (deeming what an individual "seeks to preserve as private, even in an area accessible to the public," as "constitutionally protected").

68. *See Smith*, 442 U.S. at 742.

69. *See id.* at 743.

70. *See id.* at 745–46.

Additionally, the Court dismissed any property claim by the individual.[71] Considering that the pen register was installed and used on the telephone company's property, the individual could not claim that the police invaded any constitutionally protected area because there were no applicable property rights.[72] Further, the Court distinguished the pen register from the listening device in *Katz* because a search with the former cannot provide the contents of communications or even distinguish whether a communication ever existed.[73] Overall, the Court found that any individual who voluntarily dials a phone number on his telephone assumes the risk of disclosure because he lacks a reasonable expectation of privacy in the dialed number.[74] Even if an expectation of privacy was individually harbored, it is not legitimate.[75]

3. Criticisms of the Third-Party Doctrine

Throughout the evolution of the third-party doctrine, it has been subjected to much criticism. Justice Thurgood Marshall wrote a dissent in *Smith*, discussing relevant privacy factors intertwined within the third-party doctrine.[76] At the very basis of the doctrine, Justice Marshall was not convinced that individuals know that the phone calls they make are monitored by phone companies for internal purposes or, more specifically, that such information can be made available to the public or the government.[77] Justice Marshall suggested that the Court was misguided in holding that individuals have "assumed the risk" of governmental disclosure for two reasons: (1) it is unreasonable to state that an individual has assumed the risk when there are no realistic alternative choices and (2) making risk analysis dispositive in determining what is a reasonable privacy expectation allows the government to define the scope of Fourth Amendment protections.[78] Justice Marshall's dissent argued that such misguided conception forces individuals to assume the risk of activities most would consider daily tasks in a free and open society.[79]

Additionally, Justice Sonia Sotomayor criticized the third-party doctrine in light of modern technology in *Jones*.[80] In *Jones*, the

71. *See id.* at 741.
72. *Id.*
73. *Id.*
74. *Id.* at 744.
75. *Id.* at 745.
76. *Id.* at 749 (Marshall, J., dissenting).
77. *Id.*
78. *Id.* at 749–50 (quoting *id.* at 744–45 (majority opinion)).
79. *See id.* at 750.
80. *See* United States v. Jones, 565 U.S. 400, 413–14 (2012) (Sotomayor, J., concurring).

government placed a GPS tracking device on an individual's vehicle to track his movements for a period of four weeks, all without his consent or a warrant.[81] The Court found, and Justice Sotomayor agreed, that such intrusion on his privacy was a violation of the Fourth Amendment.[82] The majority opinion relied on a trespassory test to determine if the search violated the Fourth Amendment.[83] Under the test, the Fourth Amendment only protects against searches with regard to the enumerated persons, houses, papers, and effects.[84] Thus, the *Katz* reasonable expectation of privacy test and the common law trespassory test laid out in *Jones* work together to form a doctrinal examination of Fourth Amendment search violations.[85] However, Justice Samuel Alito argued that the current doctrinal examination of Fourth Amendment searches may begin to exclude many types of surveillance that lack physical intrusion.[86] With electronic surveillance and nontrespassory circumstances increasing rapidly, it becomes difficult to ascertain if the common law trespassory test applies or whether the Court must turn to *Katz* for situations involving mere transmission of electronic signals. The majority in *Jones* understood that issues concerning modern technology are going to affect how Fourth Amendment search violations are examined; however, it provided no resolution for these pressing issues.[87]

Further, Justice Sotomayor touched on the privacy issues regarding the GPS surveillance used in Jones's vehicle.[88] She explained that the GPS monitoring raises privacy concerns under the Fourth Amendment because it "generates 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."[89] Such low-cost monitoring is an invasion of one's most intimate aspects of life and expectation of privacy.[90] Additionally, permitting such GPS monitoring impairs the checks on law enforcement used to prevent abusive police practices.[91] Due to a lack of regulation of police officers and easy access

81. *Id.* at 403 (majority opinion).

82. *Id.* at 413 (Sotomayor, J., concurring) ("[A] search within the meaning of the Fourth Amendment occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area.'" (second alteration in original) (quoting *id.* at 406 n.3 (majority opinion))).

83. *See id.* at 411 n.8 (majority opinion).

84. *See id.*

85. *See id.* at 414 (Sotomayor, J., concurring).

86. *See id.* at 427 (Alito, J., concurring).

87. *See id.* at 412–13 (majority opinion).

88. *See id.* at 416 (Sotomayor, J., concurring).

89. *Id.* at 415.

90. *See id.* at 416.

91. *Id.* at 415–17.

to low-cost surveillance, Justice Sotomayor argued that GPS monitoring should potentially be highly regulated under the Fourth Amendment because of how intrusive it is on one's personal life, especially when an individual does not expect the government to obtain such information.[92]

Some scholars dive into what the word "expectation" necessarily means with regards to the *Katz* reasonable expectation of privacy test.[93] Justice Harlan explained that a "subjective" expectation of privacy is not applicable because it cannot add to or detract from an individual's Fourth Amendment claim.[94] This is proven by the second part of the rule, which demands that such expectation be both reasonable and one that society is prepared to recognize as such.[95] Therefore, it is argued that *Katz* and the Fourth Amendment "tell us what we should demand of the government."[96] Because of such controversy about the meaning of the rule itself, it has been difficult for the Court to estimate, and subsequently make decisions on, activities of the police considering that most of what they do is not specifically authorized by law.[97] This uncertainty of the law is not only frustrating for individuals and police officers but is also "frightening" for the Court to estimate, specifically when it comes to ruling on cases concerning electronic data in the new digital age—where the doctrinal rule is quite muddled.[98] As one scholar put it, the "rapid technology advances . . . have underlined the possibility of worse horrors yet to come."[99]

---

92. *Cf. id.* at 416–18 ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." (citations omitted)).

93. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) (assessing what the word "expectation" means in the *Katz* test considering that the term is not used in the opinion).

94. *See id.*; *see also* Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2014) (claiming that there is only one step to the *Katz* test because subjective expectations are irrelevant).

95. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

96. Amsterdam, *supra* note 93, at 384.

97. *Id.* at 386.

98. *See id.*

99. *Id.*

To that end, many other scholars have also criticized how easily the government overcomes such an expectation of privacy.[100] This ease of overcoming the law is furthered by advancements in technology because larger quantities of private information are being shared with the government without repercussion.[101] Overall, technological advancements continue to complicate what the third-party doctrine governs. Although the *Katz* opinion considered technological advancements, it simply was not enough to guide the Court going forward.[102] In fact, since *Katz*, it has been difficult for the Court to determine how the Fourth Amendment applies to electronic communications and digital information.[103]

II. *CARPENTER V. UNITED STATES*: NEWEST APPROACH TO THE THIRD-PARTY DOCTRINE

Fourth Amendment rights are continuously interpreted as new facts and instances are discovered in cases such as *Carpenter v. United States.* This section will discuss *Carpenter* in its entirety as it refers to not only Fourth Amendment rights, but how it does *not* appeal to the third-party doctrine. Realizing why this case is so vital to criminal procedure moving forward stems from understanding why the Supreme Court initially granted certiorari, and how its holding effects the way in which courts will discuss Fourth Amendment third-party issues. This section will not only explain the *Carpenter* case but will also reflect upon how the Supreme Court left the third-party doctrine in a state of disarray with its lack of guidance on such relevant issues.

A. *Why the Supreme Court Granted Certiorari*

In 2011, four men were arrested for a series of robberies of Radio Shack and T-Mobile stores across Detroit.[104] One of the men confessed to the robberies and implicated the three others along with fifteen accomplices, most of whom he provided cell phone numbers for.[105] Prosecutors requested court orders to obtain cell phone records for each of the men arrested and their accomplices under the Stored

100. Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 262 (2016).

101. *See id.*

102. *See id.* at 263–64.

103. *Id.* at 264.

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

105. *Id.*

Communications Act.[106] Subsequently, a federal magistrate judge issued two court orders directing MetroPCS and Sprint to disclose all of Carpenter's CSLI for call origination and termination during the four-month period in which the robberies occurred.[107] Collectively, the government obtained 12,898 location points from the cellular carriers, which effectively placed Carpenter near the scene of the robberies.[108] Carpenter was arrested and charged with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[109] He moved to suppress the CSLI, arguing that obtaining the records was a clear violation of his Fourth Amendment right to privacy because the police needed a warrant, rather than a court order, under the Stored Communications Act.[110] The U.S. Court of Appeals for the Sixth Circuit affirmed the denial of the defendants' motion to suppress the CSLI.[111] It held that Carpenter had no reasonable expectation of privacy in the CSLI because he voluntarily shared it with his wireless carrier.[112] The court considered the CSLI business records, which do not receive Fourth Amendment protection.[113] After rehearing en banc was denied in June of 2016,[114] the Supreme Court granted certiorari to hear *Carpenter* on June 5, 2017.[115] The defendants, Timothy Ivory Carpenter and Timothy Michael Sanders, brought the case to the Supreme Court to answer one question: whether accessing historical cell phone records that provide a comprehensive chronicle of the user's past movements is a violation of an individual's Fourth Amendment right to privacy.[116]

Additionally, it is important to note exactly where this CSLI comes from. At trial, a Federal Bureau of Investigation (FBI) agent provided expert testimony explaining how agents make "maps" out of the recorded information.[117] Every time a cell phone connects to a wireless network, a time stamp is logged with the carrier, which records the particular cell

106. *Id.*; *see also* 18 U.S.C. § 2701 (2018) (making it an offense to intentionally access a facility that provides electronic communication services without prior authorization); *id.* § 2703(d) (requiring a court order for any governmental agency to receive such stored communications).

107. *Carpenter*, 138 S. Ct. at 2212.

108. *See id.*

109. *Id.*

110. *Id.*

111. *Id.* at 2213.

112. *Id.*

113. *See id.*; *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (explaining that telephone companies make records of relevant information for legitimate business purposes, which essentially makes them business records).

114. United States v. Carpenter, 2016 U.S. App. LEXIS 13024 (6th Cir. June 29, 2016).

115. Carpenter v. United States, 137 S. Ct. 2211 (2017).

116. *See Carpenter*, 138 S. Ct. at 2211.

117. *Id.* at 2212–13.

cite and sector used.[118] Essentially, every time an individual uses his cell phone, a stamp is placed on his network that records the location of the cell tower used to make the phone call. CSLI can provide near-perfect surveillance—ranging from one-eighth to four square miles—and can be traced back up to five years.[119] However, because of modern technology, wireless carriers can now pinpoint a phone's location within fifty meters by calculating the time and range in which cell towers are struck.[120] Because of such information, the FBI agents were able to make "maps," which placed Carpenter's phone near the location of the robberies.[121]

B. *The Holding and its Effect on the Third-Party Doctrine*

The *Carpenter* decision itself is narrow and does not disturb the applicability of *Smith* or *Miller*, nor does it call into question conventional surveillance techniques and tools, such as security cameras.[122] Due to the Court's finding that obtaining CSLI from a wireless carrier is a violation of Fourth Amendment privacy concerns, it is now necessary to obtain a warrant subject to probable cause before acquiring such records.[123] Thus, prosecutors may no longer obtain court orders under the Stored Communications Act to obtain CSLI from wireless carriers because the Act only requires "reasonable grounds," rather than probable cause, to show relevance for the records.[124] With regard to the third-party doctrine, the Court determined that if "modern-day equivalents of an individual's own 'papers' or 'effects'" do not fall under any protected category under the doctrine, then full Fourth Amendment protection should apply.[125] The Court further attempted to narrow its ruling by explaining that such warrant requirement only applies when an individual "has a legitimate privacy interest in records held by a third party."[126] Exceptions to the rule, however, do apply. The government may conduct a warrantless search of CSLI if exigent circumstances apply, including protecting individual safety, being in the act of hot pursuit, or preventing imminent destruction of evidence.[127]

---

118. *Id.* at 2212.
119. *See id.* at 2218.
120. *Id.* at 2219.
121. *Id.* at 2213.
122. *Id.* at 2220.
123. *See id.*
124. *Id.* at 2221 (quoting 18 U.S.C. § 2703(d) (2012)).
125. *Id.* at 2222 (quoting *id.* at 2230 (Kennedy, J., dissenting)).
126. *Id.*
127. *Id.* at 2222–23; *see, e.g.*, Kentucky v. King, 563 U.S. 452, 455 (2011) (preservation of evidence exception); Brigham City v. Stuart, 547 U.S. 398, 400 (2006) (safety exception);Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring) (hot pursuit exception).

Although this case could have provided a massive and necessary reconstruction of the third-party doctrine in the face of modern technology, it failed to do so. As the Court explained, the decision is very narrowly tailored to answer the specific question at issue, which only concerned CSLI records obtained from a cellular or wireless carrier without probable cause for a warrant.[128] The largest remaining concern is that the Court failed to explain how this case fits in with the third-party doctrine, especially considering that it does not disturb the application of *Smith* or *Miller*.[129] Some scholars claim that this case is merely an extension of *Katz* and *Smith*, explaining that because telephone booths are essentially extinct, the growing expectation of privacy in modern technology, such as cell phones, must be afforded Fourth Amendment protection.[130] However, the Court did not explicitly, or implicitly for that matter, claim such an extension of existing precedent, but it did claim that *Carpenter* in no manner affects the overall outcome of *Smith* or *Miller*.[131] Just because the types and uses of telephones have evolved over time, it does not follow that the underlying concept of voluntarily giving information to a third party must differ as a result.[132] So long as the concept remains the same, so should the doctrinal process governing it.

A series of dissents expressed *Carpenter*'s many implications for the third-party doctrine. Justice Anthony Kennedy explained that the Court's decision will have ramifications that extend far beyond cell-site records considering that it failed to provide clear guidelines for law enforcement to follow.[133] He also pointed out that the Court failed to explain what makes something a distinct category of information such as bank and phone records.[134] Law enforcement must estimate which records they are permitted to obtain prior to getting a warrant, so long as there are no clear guidelines directing them on such distinct categories of information.[135] By not implementing *Carpenter* into the set precedent of *Smith* and *Miller*, the Court effectively led the future of the third-party doctrine

128. *See Carpenter*, 138 S. Ct. at 2220–21.

129. *See id.* at 2220.

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

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

132. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Causation*, 102 MICH. L. REV. 801, 828 (2004) ("New technologies commonly expose information that in the past would have remained hidden, resulting in meager Fourth Amendment protection in new technologies."). *But see* Gelb, *supra* note 130, at 36.

133. *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting).

134. *Id.*

135. *See id.*

down an "uncharted course," forcing judges and defendants into "guessing for years to come."[136]

On another note, Justice Clarence Thomas and Justice Samuel Alito both explained the importance of recognizing when document possession rests with a party other than the defendant.[137] Justice Thomas claimed that Carpenter did not have any reasonable expectation of privacy in the cell-site records because the government obtained records that were created, maintained, and controlled solely by MetroPCS and Sprint, not Carpenter.[138] Justice Thomas further elaborated that the *Katz* test should have no basis within the Fourth Amendment because it confronts policy instead of law.[139] Essentially, he argued that the *Katz* test undermines the entirety of a person's Fourth Amendment protections because it changes the meaning of the word "search."[140] Justice Alito added that the Fourth Amendment does not protect the persons, houses, papers, and effects of others—such right is an individual right.[141] He argued that requiring probable cause to obtain cell-site records is a mistake simply because the documents were ordered by a functional equivalent of a court subpoena without any evidence of a "search."[142] The Court ignored basic distinctions between an actual Fourth Amendment "search" and a search of a party's own private records through the production of specific documents.[143] Searching a party's private records is only a search of an individual's own source of information and thus does not require probable cause.[144] Justice Alito further explained that the Court failed to follow *Oklahoma Press Publishing Co. v. Walling*,[145] which states that "a showing of probable cause [is] not necessary so long as" Congress properly authorizes the investigation "and the documents sought are relevant."[146] The records received in *Carpenter* were under court order from the government and thus should have been immune from any Fourth Amendment challenges.[147]

136. *Id.* (quoting Riley v. California, 573 U.S. 373, 401 (2014)).

137. *See id.* at 2235 (Thomas, J., dissenting); *id.* at 2257 (Alito, J., dissenting).

138. *See id.* at 2235 (Thomas, J., dissenting).

139. *Id.* at 2236.

140. *See id.* at 2238 (explaining that *Katz* defines "search" to mean "any violation of a reasonable expectation of privacy," whereas the Fourth Amendment intends to protect against violations of unreasonable searches).

141. *Id.* at 2257 (Alito, J., dissenting).

142. *See id.* at 2247.

143. *Id.*

144. *See id.*

145. 327 U.S. 186 (1946).

146. *Carpenter*, 138 S. Ct. at 2254 (Alito, J., dissenting).

147. *Id.* at 2255.

Subsequently, Justice Neil Gorsuch argued that people today use the internet and smartphones for almost everything.[148] Thus, *Smith* and *Miller* are relevant but no longer have a clear reach or meaning.[149] Justice Gorsuch argued that the Court's balancing inquiry—asking whether disclosure to a third party outweighs privacy interests—inevitably stemmed from *Katz*, but does nothing more than provide a more weighty analysis with little guidance.[150] He introduced the idea that accessing and possessing records can be a type of legal bailment by exploring doubt that exclusive control of property is necessary to assert a Fourth Amendment right.[151] This differs completely from the customary property rights shown in *Smith* and *Miller* considering that all Fourth Amendment rights are extinguished upon transfer of the property to a third party.[152] However, Justice Gorsuch argued that individuals should not have to lose all Fourth Amendment rights simply because they are forced to hand over their information to a third party.[153] Modern technology complicates these concepts—morphing black letter law into questionable determinations with an unsettled pathway. Cases such as *Carpenter* are important not only for understanding the basis of the third-party doctrine but also for keeping the Court current with modern technology. Failure to do so makes it difficult to conceptualize the law, especially when the most up-to-date case fails to consider the loopholes created by modern technology.

Admittedly, it is difficult for Justices to draft an opinion that encompasses all possible issues. However, it is important for the Court to at least address the most pressing issues surrounding the case at hand. In *Carpenter*, the most pressing issues were (1) whether Carpenter's CSLI was illegally obtained from his provider violating his Fourth Amendment rights and (2) how the exact ruling would fit in with the current third-party doctrine, including *Smith* and *Miller*.[154] The Court specifically stated that its opinion did not affect *Smith* and *Miller*, which is an oversight likely to cause disarray in the lower courts due to lack of guidance.[155] The Court claimed that it failed to extend *Smith* and *Miller* to *Carpenter* because the "unique nature" of the CSLI made it more

148. *Id.* at 2262 (Gorsuch, J., dissenting).

149. *See id.* at 2267.

150. *Id.*

151. *See id.* at 2268–69.

152. *See id.* at 2269.

153. *Id.* at 2270.

154. *Id.* at 2211 (majority opinion); Eunice Park, *Protecting the Fourth Amendment After* Carpenter *in the Digital Age: What Gadget Next?*, ORANGE COUNTY L. MAG., May 2018, at 35, 35 ("[T]he Court's holding in *Carpenter* and how it arrives at it will have significant repercussions for lower courts trying to address the next Fourth Amendment technology-based challenges.").

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

intrusive on an individual's Fourth Amendment rights than phone or bank records.[156] However, such information is no more intrusive than obtaining an individual's log of phone calls or complete bank records. Considering that *Smith* and *Miller* are the basis of the third-party doctrine, it is difficult to understand why the Court did not follow precedent and why this new ruling did not affect these cases. Failing to answer these questions in a clear and concise manner only leaves confusion for the lower courts and police officers attempting to follow the law when obtaining similar information. Chief Justice John Roberts had the opportunity to write a significant opinion regarding the nature of the third-party doctrine but instead drafted one that made dense law even more difficult to follow.

III. IMPLICATIONS OF THE *CARPENTER* DECISION—WHAT IS NEXT?

There are three possible options for fixing the limitations of *Carpenter*. First, the Supreme Court can collectively determine that it properly decided *Carpenter* and thus remain with the current law. Even if the Court chooses this option, it should at least complete a thorough review of the case. Second, individuals can call for legislative action to determine how these new technological advances affect the legal system. Considering that increased technology has drastically affected the understanding of the third-party doctrine, it may be necessary for the legislature to rectify these issues. Lastly, the Supreme Court could reverse its decision in *Carpenter*, agreeing that the technology at issue in the case was not as advanced as the Court attempted to make it seem.

A. *Remain with* Carpenter

Although the Court drafted a dense opinion regarding the pressing question of placing CSLI within the parameters of the legal system, it did not thoroughly render the decision. Instead of placing this case, among many others, under the third-party doctrine, the Court distinguished it from the doctrine and required a warrant for obtaining information held by a third party.[157] Effectively veering away from this well-known doctrine provides a state of uncertainty as to what exactly does fall under the doctrine and what does not. After all, like in *Smith*, the Court admitted that telephone subscribers are aware that the numbers they dial are used for a variety of business purposes and thus voluntarily consent to such information being exposed in the ordinary course of business.[158] However, the Court somehow concluded that even though the third-party

156. *Id.*
157. *See id.* at 2221.
158. *Id.* at 2216.

principles of *Smith* and *Miller* were implicated, that is not enough to overcome Fourth Amendment protection.[159] The Fourth Amendment undermines that conclusion because it only protects against physical intrusions of one's body or property, which does not extend to that of a third party.[160] Without physical intrusion on an individual's personal property, the Fourth Amendment protection does not apply and should remain subject to a *Katz* interpretation.[161]

Carpenter is extremely similar to the well-established precedent of *Smith*, which has effectively formed the third-party doctrine into what it is today.[162] If the CSLI technology was created, installed, and used on service provider property, then Carpenter should not be able to claim his property was invaded or unconstitutionally intruded upon—because it was never his property in the first place.[163] Carpenter did not form this technology, nor did he assist in forming the information other than by making the calls.[164] He simply dialed phone numbers, which the Court previously classified as business records subject to the third-party doctrine.[165]

The Court in *Carpenter* countered this argument by stating that *Smith* pointed out that pen registers reveal little identifying information,[166] while claiming that CSLI entails a "detailed chronicle of a person's physical presence."[167] This argument, however, was proven invalid when the government explained that such information, taken from the cell phone, was less precise than GPS information because it only places the location "within a wedge-shaped sector ranging from one-eighth to four square miles."[168] In no plausible manner can the CSLI pulled from a cell phone be equivalent to that of GPS monitoring. It is true that when the government tracks the location of a cell phone it can achieve a near-

159. *Id.* at 2217.

160. U.S. CONST. amend. IV.

161. United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring); *see also* Katz v. United States, 389 U.S. 347, 349–50 (1967) (recognizing that the proper Fourth Amendment inquiry cannot focus solely on physical intrusion); Christian Bennardo, Note, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 FORDHAM L. REV. 2385, 2411–12 (2017) (explaining that the trespass-based approach of the Fourth Amendment is inapplicable to cases such as *Jones*, considering that there is no physical intrusion involved with CSLI).

162. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979).

163. *Cf. id.* at 742.

164. *Cf. Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).

165. *See Smith*, 422 U.S. at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.").

166. *Carpenter*, 138 S. Ct. at 2219.

167. *Id.* at 2220.

168. *Id.* at 2218.

perfect surveillance; however, that was not the issue or what the government did in *Carpenter*.[169] After all, CSLI is only a collection of time stamps placed on a cell phone considered incidental to finding the best signal in that particular location.[170] Each time a signal is found, the cell phone records it in order for the user to make a phone call or send a text message.[171] So, technically, a user does in fact assume the risk of his physical movements being tracked by the government because he voluntarily places that information in his service provider's hands.[172] However, the physical movements the Court attempts to portray as "GPS" are nothing more than the location of a series of cell phone towers.

Holding that time stamps from cell towers are anything other than an incidental result of providing effective telephone service undermines the validity of the third-party doctrine. Considering the many inconsistencies and varying legal dilemmas within *Carpenter*, why should the Court keep an opinion in place that only confuses the legal system and the citizens who must abide by it? The answer is simple, it should not.

B. *Ask for Legislative Action*

Instead of the judicial system determining how these technological advances affect privacy rights, it is possible to leave this issue for the legislature to decide. This could be done by acknowledging that one's constitutional right to privacy is at stake, but technological advances have made it nearly impossible for the judicial system to resolve that privacy concern without implicating other branches of the government. Thus, the question could become nonjusticiable due to its political nature.[173]

The right to privacy is essentially the right to personal autonomy. Although the Constitution does not explicitly provide for the right to privacy or for a general right to personal autonomy, the Supreme Court has repeatedly ruled that a right to personal autonomy is implied in the "zones of privacy" created by specific constitutional guarantees.[174] These

169. *Id.*

170. *See id.* at 2211.

171. *See id.*

172. *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (explaining that a telephone user assumes the risk of information disclosure because he voluntarily conveys the information in the ordinary course of business); *see also* United States v. Jones, 565 U.S. 400, 430–31 (2012) (Alito, J., concurring) (explaining that it is best to apply Fourth Amendment protection and ask whether GPS tracking is more intrusive than reasonably anticipated).

173. *See* John Harrison, *The Political Question Doctrines*, 67 AM. U. L. REV. 457, 528 (2017) (explaining that the political question doctrine tells courts how to decide cases, which then leaves individual jurisdictions to decide for themselves how to resolve disputes).

174. Alex Alben, *"Reasonable Zones of Privacy"—The Supreme Court's Struggle to Find Clarity in the American Landscape Regarding Fourth Amendment Rights*, 12 WASH. J.L. TECH. & ARTS 145, 147 (2017) (explaining that zones of privacy have evolved over time but essentially

zones of privacy were created in multiple aspects of the Bill of Rights, which the Founders intended as further protection to U.S. citizens against government.[175] Due to increased technological advances, individuals attempt to expand this concept of privacy to find such protection in a modern world.[176] However, these limits cannot exceed due process protection. Thus, when attempting to expand these privacy limits, it is necessary to ask whether the government has an adequate reason for taking away a person's life, liberty, or property.[177] In *Carpenter*, the issue was whether an individual has a privacy interest in CSLI held by cell phone providers.[178] To be covered by constitutional zones of privacy, it must be determined that such privacy concern is a fundamental right[179] or liberty. The constitutional standard for determining if a right is fundamental is often dictated by *Palko v. Connecticut*.[180] In that case, the Court noted that fundamental rights are something objectively and deeply rooted in this nation's history and tradition.[181] Further, the right must be implicit in the concept of ordered liberty such that neither liberty nor justice would exist if the right was sacrificed.[182] However, tradition can be a tricky concept. Tradition is a living, breathing thing and acts as a rational continuum, which broadly includes a freedom from all

---

define what rights are protected under the Fourth Amendment); *see also* Whalen v. Roe, 429 U.S. 589, 598–600 (1977) (discussing the concept of zones of privacy as it relates to certain important personal decisions).

175. *See* Isidore Silver, *The Future of Constitutional Privacy*, 21 ST. LOUIS U. L.J. 211, 216–17 (1977).

176. *See id.* at 222–24 ("Privacy is unique in that it derives little independent protection by precedent and none from the text of the Constitution while, paradoxically, it is recognized as a fundamental social value.").

177. *See Substantive Due Process*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("The doctrine . . . require[s] legislation to be fair and reasonable in content and to further a legitimate governmental objective.").

178. *See supra* notes 107–10 and accompanying text

179. *See Fundamental Right*, BLACK'S LAW DICTIONARY, *supra* note 177 ("A right derived from natural or fundamental law.").

180. 302 U.S. 319 (1937), *overruled by* Benton v. Maryland, 395 U.S. 784 (1969).

181. *See id.* at 325 (finding that a right is not fundamental where its abolition does not "violate a 'principle of justice so rooted in the traditions and conscience of our people as to be ranked as fundamental'" (first quoting Snyder v. Massachusetts, 291 U.S. 97, 105 (1934), *overruled in part by* Malloy v. Hogan, 378 U.S. 1 (1964); then quoting Brown v. Mississippi, 297 U.S. 278, 285 (1936); and then quoting Herbert v. Louisiana, 272 U.S. 312, 316 (1926))); *see also* Washington v. Glucksberg, 521 U.S. 702, 720–21 (1997) ("[W]e have regularly observed that the Due Process Clause specially protects those fundamental rights and liberties which are, objectively, 'deeply rooted in this Nation's history and tradition,' and 'implicit in the concept of ordered liberty,' such that 'neither liberty nor justice would exist if they were sacrificed.'" (citations omitted) (first quoting Moore v. East Cleveland, 431 U.S. 494, 503 (1977) (plurality opinion); and then quoting *Palko*, 302 U.S. at 325, 326)).

182. *Palko*, 302 U.S. at 324–26.

substantial arbitrary impositions and purposeless restraints.[183] Thus, employing tradition alone to determine whether a right is fundamental does not provide jurisprudence with much certainty.[184]

It is well established that individuals have a constitutional right to privacy regarding their persons, houses, papers, and effects.[185] *Carpenter* expanded such constitutional right to encompass an individual's CSLI obtained from his cell service provider.[186] Thus, the Court determined that CSLI is personal and private to the individual, which grants full protection under the Fourth Amendment.[187] In doing so, the Court simply determined that an individual held privacy rights in the information but failed to discuss whether such information was implicit in the ordered concept of liberty or rooted in tradition. Accordingly, scholars have argued that if CSLI protection does not fall under the third-party doctrine as the Court determined, it should be left for the legislature to decide.[188] Because of these disparities, it may be best to grant the legislature the opportunity to analyze expert opinions, expert testimony, and public opinion on an equal playing field while balancing important government interests.[189] The Court failed to explain why it categorized CSLI under the fundamental right to privacy blanket so quickly. Thus, it may be reasonable to consider CSLI protection as a political question.

A political question is not suitable for judicial resolution because it is more suitable for congressional review. There are two strands of the modern political doctrine: (1) textual (some matters are committed to the unreviewable discretion of the political branches) and (2) prudential (some otherwise legal questions ought to be left to the other branches as a matter of prudence).[190] The standard for the political question doctrine is the *Baker v. Carr*[191] evidence test, which uses six factors to determine

183. Poe v. Ullman, 367 U.S. 497, 543 (1961); *see also* Griswold v. Connecticut, 381 U.S. 479, 501 (1965) (Harlan, J., concurring) ("[Judicial self-restraint] will be achieved in this area, as in other constitutional areas, only by continual insistence upon respect for the teachings of history . . . .").

184. *See* Adam B. Wolf, *Fundamentally Flawed: Tradition and Fundamental Rights*, 57 U. MIAMI L. REV. 101, 154 (2002).

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

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

187. *See id.*

188. *See* Samantha G. Zimmer, Student Article, *Cell Phone or Government Tracking Device?: Protecting Cell Site Location Information with Probable Cause*, 56 DUQ. L. REV. 107, 125–26 (2018) (claiming that the Supreme Court is not the only implicated body when authorizing the definition and placement of CSLI within Fourth Amendment protection and that the legislature should take issue with CSLI).

189. *Id.* at 136.

190. Zachary Baron Shemtob, Note, *The Political Question Doctrines:* Zivotofsky v. Clinton *and Getting Beyond the Textual-Prudential Paradigm*, 104 GEO. L.J. 1001, 1002 (2016).

191. 369 U.S. 186 (1962).

whether a question is political in nature.[192] Only one of these factors needs to be met to consider the question nonjusticiable.[193] With regard to the question of CSLI protection, there is currently a lack of judicially discoverable and manageable standards resolving such issue.[194] Although the Supreme Court has attempted to resolve the issue, it failed to recognize that CSLI is no more than ordinary business records held by the service provider and to consider future technological advances that will continuously poke at the current third-party doctrine. Therefore, Congress may be able to provide a statutory resolution that offers a more precise and uniform standard that courts and citizens can effectively rely upon and understand.[195]

C. *Reverse* Carpenter

Although legislation may be a valid option that would effectively provide a standardized resolution for technological advancements under the right to privacy, this issue should continue to remain within the judicial system. The third-party doctrine has been around since the 1970s and courts have effectively handled privacy issues regarding the Fourth Amendment in a clear and concise manner—until *Carpenter*. Although it may take some time, the Court has the ability to both reverse *Carpenter* and determine that not all technological advances amount to an infringement upon one's Fourth Amendment rights. Although technology poses a continuing threat to individual privacy,[196] certain aspects of life

192. *See id.* at 217.

193. *See id.* ("Prominent on the surface of any case held to involve a political question is found a textually demonstrable constitutional commitment of the issue to a coordinate political department; or a lack of judicially discoverable and manageable standards for resolving it; or the impossibility of deciding without an initial policy determination of a kind clearly for nonjudicial discretion; or the impossibility of a court's undertaking independent resolution without expressing lack of the respect due coordinate branches of government; or an unusual need for unquestioning adherence to a political decision already made; or the potentiality of embarrassment from multifarious pronouncements by various departments on one question.").

194. *Id.*

195. Zimmer, *supra* note 188, at 136–37.

196. *See, e.g.*, Jemima Kiss, *Does Technology Pose a Threat to Our Private Life?*, GUARDIAN (Aug. 20, 2010, 7:06 PM), https://www.theguardian.com/technology/2010/aug/21/facebook-places-google [https://perma.cc/PC6Z-6ZXW] ("The rapid pace of development by technology companies often throws up new cultural and ethical challenges."); Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/ [https://perma.cc/6Y84-9549] ("[E]ffective laws and standards of ethics are guidelines accepted by members of a society, and . . . these require the development of a social consensus."); Colin Wood, *Rethinking Privacy: Though Technology Has Outspaced Policy, That's No Reason To Give Up*, GOV'T TECH. (June 2, 2014), http://www.govtech.com/data/Rethinking-Privacy-Though-Technology-has-Outpaced-Policy-Thats-No-Reason-to-Give-Up.html [https://perma.cc/

must remain subject to police observation to protect people from criminal conduct.[197] For instance, scholar Herbert Packer published *Two Models of the Criminal Process* in 1964, which established two theoretical models of justice for criminal law: the crime-control model and the due process model.[198] "The crime-control model attempts to achieve maximum efficiency in the repression of criminal conduct," whereas the due process model finds administrative restrictions necessary to prevent individual suppression.[199] As a whole, the models provide a guide to operating the criminal justice system.[200] The models are often categorized as two "extremes" of the law, finding most individuals' ideological beliefs resting somewhere in the middle of the two concepts.[201] The crime-control model offers a presumption of guilt in adjudication, whereas the due process model more so provides a presumption of innocence.[202] Considering that the crime-control model is based on societal interests in security, there is an underlying assumption in criminal law that individuals want to be protected.[203] Of course, this extreme view must be balanced with due process and individual rights in relation to the state.[204] This concept seems rather easy—the Court should make and interpret laws to protect individuals from criminal activity and to ensure that their privacy rights in relation to the state will not be infringed upon. However, this concept is easier said than done, especially when including continuous technological advances.

CSLI is a collection of time stamps placed on a cell phone from towers picking up its signal and converting such energy into a telephone call or a text message.[205] Without such signal, the cell phone simply would not work, rendering the phone useless. The *Carpenter* Court found that accessing this information was an improper infringement on an individual's privacy rights. However, not only is such information a

---

J4BC-6TA2] ("Privacy is almost universally valued by humanity, but technology is advancing so quickly that people haven't even had time to settle on a useful definition for the word, let alone a solution that everyone can live with.").

197. *See* Belinda R. McCarthy, *Case Attrition in the Juvenile Court: An Application of the Crime Control Model*, 4 JUST. Q. 237, 238 (1987).

198. Herbert Packer, *Two Models of the Criminal Process*, 113 U. PA. L. REV. 1, 6 (1964); *see* McCarthy, *supra* note 197, at 238.

199. McCarthy, *supra* note 197, at 238.

200. Kent Roach, *Four Models of the Criminal Process*, 89 J. CRIM. L. & CRIMINOLOGY 671, 672 (1999).

201. *See, e.g.*, Vanessa A. Edkins & Kenneth D. Royal, *Evaluating the Due Process and Crime Control Perspectives Using Rasch Measurement Analysis*, 7 J. MULTIDISCIPLINARY EVALUATION 48, 50 (2011).

202. *See id.*

203. *See* Roach, *supra* note 200, at 672.

204. *Id.*

205. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

compilation of data that the phone company created to ensure efficient telephone service, it also provides an effective means for police officers to narrow their searches of individuals suspected of criminal or fraudulent activity. This technological advancement is not accurate enough to consider it a precise pinpoint location of an individual's whereabouts, as it does not equate to GPS.[206] Additionally, information of this type has long been used as an effective means for police officers to locate and charge dangerous criminals.[207] The ability of police officers to obtain information that does not infringe on individual privacy any more than ordinary business records already subject to government intrusion is necessary for maintaining order and safety in society. It should be looked at not as a means of infringement but as a means of possible protection.

However, just as the two models of criminal process illustrate,[208] there will always be two extremes to the law. True balance stems from a democratic-style government because society balances itself out. It is possible for the government to step too far into individual privacy rights when it is not necessary or proper to do so. There must be a limit to government power, but there must also be room for the government to do its job. One job is to protect its citizens, but another is to incarcerate criminals who undertake illegal behavior. CSLI is convoluted because it provides information to the government that individuals have not had to worry about in the past—simply because such information was not feasible to obtain. However, advancement of technology does not, and should not, automatically render newfound information unconstitutionally searched or seized. Fourth Amendment protection is essential and serves as an outstanding guideline for privacy rights, but it only applies when one's life, liberty, or property is at stake.[209]

This protection does not extend to records held by a third party.[210] Carpenter did not create the CSLI obtained by the police and should not be permitted to claim such information as his personal property. He simply dialed phone numbers, which provided the police with information relating to which cell tower his cell phone used to obtain signal.[211] The information taken from the cell phone provider was less precise than gatherings of GPS information because it only placed the

206. *Contra id.* at 2219–20 (claiming that the tracking in *Carpenter* equated to "a detailed chronicle of a person's physical presence").

207. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 737 (1979) (using a pen register to record dialed phone numbers to track down a man continuously making threatening phone calls to a woman whom he previously robbed).

208. *See supra* notes 198–204 and accompanying text.

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

210. *See supra* notes 33–35 and accompanying text.

211. *See Carpenter*, 138 S. Ct. at 2212.

location "within a wedge-shaped sector ranging from one-eighth to four square miles."[212] The government did not extract the location of the cell phone itself but a range of space in which the user of the cell phone had dialed phone numbers to make phone calls.[213] Without the ability of the cell towers to grant a user signal, the individual would not be able to make a phone call. *Carpenter* is not a matter of privacy issues relating to "tracking" an individual through his cell phone; rather, it is an argument over which business records the Court deems accessible. This issue was resolved over fifty years ago and should remain binding on the Court until a more pressing and intrusive violation of an individual's Fourth Amendment rights is at stake. As a matter of doctrinal proceedings, it is important to follow precedent when applicable. The third-party doctrine set out in *Smith* and *Miller* provides an adequate remedy for *Carpenter* because the time stamps (or CSLI) are nothing more than business records held in the ordinary course of a service provider's business of providing effective cell service to its users.

CONCLUSION

The Supreme Court granted certiorari in *Carpenter v. United States* to resolve a privacy issue concerning CSLI, which happens to be quite the technological advancement since the beginning of the third-party doctrine.[214] However, the Court released a narrow opinion failing to answer many questions concerning the state of the third-party doctrine and privacy matters concerning technology in the new digital age. The Court affirmatively answered the question of whether access to historical cell phone records providing a comprehensive chronicle of the user's past movements constitutes a search deserving protection under the Fourth Amendment.[215] However, it analogized the case far more closely to *Jones*, completely disregarding its application under *Smith* and *Miller*.[216] This case should have been decided based on how and under what circumstances such CSLI is retrieved and computed and, most importantly, why. CSLI is a collection of time stamps that attach to one's phone from an automatic connection to whichever cell tower is within the closest range.[217] The time stamps show the relative location the user was in, which is not nearly as precise as GPS tracking services.[218] The Court has previously admitted that it is not out of the ordinary for individuals

212. *Id.* at 2218.
213. *See id.*
214. *See id.* at 2211.
215. *Id.*
216. *Id.* at 2220.
217. *Id.* at 2211.
218. *See id.*

to expect their information, such as dialed telephone numbers and sent text messages, to be held by a third party for legitimate business purposes.[219] Thus, failing to recognize that time stamps on cell phones are only a means of providing effective service undermines the validity of the third-party doctrine, which has proven itself greatly effective over the past fifty years.

Fourth Amendment protection should never be disregarded when one's life, liberty, or property is at issue. But, as history has shown, that protection does not apply to records held by a third party. Voluntarily placing information in the hands of another individual effectively destroys any expected privacy. This does not change simply because the information is created by the third party, such as a log of time stamps collected from when an individual uses his phone. Extracting a range of space in which a user dialed phone numbers to make phone calls does not amount to GPS tracking simply because it narrows down the possibility of where an individual may be located. The Supreme Court resolved this issue in *Smith* and *Miller*, which have been strong precedent for about fifty years. Without more than just a disagreement over types of business records, there is no need for a radical change in the law that does nothing more than confuse the entire state of the third-party doctrine and leave police officers unaware of what they are permitted to search.

219. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).