ERECTING A PRIVACY WALL AGAINST TECHNOLOGICAL ADVANCEMENTS: THE FOURTH AMENDMENT IN THE POST-*CARPENTER* ERA

Elle Xuemeng Wang†

I. INTRODUCTION

Carpenter v. United States[1] is perhaps the "most important data privacy case of a generation."[2] Not only did this case expand the scope of Fourth Amendment searches, it also redefined the applicability of what has been considered for decades as a categorical rule—the third-party doctrine.[3]

Carpenter involved a type of information called cell-site location information. Cell-site location information is recorded by cell phone carriers' towers.[4] When a cell phone is being used, the cell phone always connects to the nearest cell tower.[5] As the user moves, the cell phone connects from tower to tower.[6] Putting together all the location information recorded by all of these towers generates a mosaic of the cell phone user's movements.[7] In *Carpenter*, without first securing a warrant, the government obtained cell-site location records from towers operated by several phone carriers.[8] Using this information, the government arrested and indicted Carpenter and several accomplices.[9] The crux of the case was whether obtaining cell-site location records constituted a search within the meaning of the Fourth Amendment.[10]

DOI: https://doi.org/10.15779/Z385T3G08H

† J.D., University of California, Berkeley, School of Law, Class of 2019.

1. 138 S. Ct. 2206 (2018).
2. Stephen Vladeck, *The Supreme Court Phone Location Case Will Decide the Future of Privacy*, MOTHERBOARD (June 16, 2017), https://motherboard.vice.com/en_us/article/59zq5x/scotus-cell-location-privacy-op-ed [https://perma.cc/5RRT-FYSA].
3. For a detailed analysis, see *infra* Section IV.A.
4. *See Carpenter*, 138 S. Ct. at 2211.
5. *See id.*
6. *See id.*
7. *See id.* at 2212.
8. *See id.*
9. *See id.*
10. *See id.* at 2212–13.

The Court reached a 5–4 decision with the majority holding that it was a search and that the third-party doctrine did not apply.[11]

While *Carpenter* was a big win for data privacy advocates, it has spurred polarized views among scholars and commentators. The Court's treatment of the third-party doctrine has especially triggered vigorous debates. Because it is unlikely that the Supreme Court will hear another data privacy case in the reasonably foreseeable future, the fate of the Fourth Amendment protections and the third-party doctrine lies in the hands of district and circuit court judges—those who will be interpreting *Carpenter*. This Note aims to provide a helpful guideline to aid district and circuit court judges with interpreting the meaning of *Carpenter* and how to apply it to future cases.

This Note will first discuss, in Part II, the landscape of the Fourth Amendment in the pre-*Carpenter* era. Part III summarizes *Carpenter*'s procedural history, the majority opinion, and dissenting opinions. Part IV interprets the majority opinion and discusses how *Carpenter*'s instructions can be applied to two technological advancements. Part V concludes.

II. LEGAL BACKGROUND AND HISTORY

The pre-*Carpenter* era is segmented by a series of seminal cases: *Boyd v. United States*,[12] *Olmstead v. United States*,[13] *Katz v. United States*, [14] and *United States v. Miller*[15]and *Smith v. Maryland*.[16] Each segment represents a significant stop in shaping the Fourth Amendment right to privacy.

A. PRE-*KATZ* ERA: UNTYING AND RETYING PRIVACY TO PHYSICAL TRESPASS

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[17] For much of its history, the Fourth Amendment was tied to common-law trespasses to persons and homes, until in 1886, Justice Bradley, for the first time, extended the protection of Fourth Amendment beyond "the sanctity of a man's home" to "the privacies of life."[18] In *Boyd*, the government attempted a warrantless seizure of thirty-five cases of glass imported by Boyd

11. *See id.* at 2223.
12. 116 U.S. 616 (1886).
13. 277 U.S. 438 (1928).
14. 389 U.S. 347 (1967).
15. 425 U.S. 435 (1976).
16. 442 U.S. 735 (1979).
17. U.S. CONST. amend. IV.
18. Boyd v. United States, 116 U.S. 616, 630 (1886).

and Son.[19] The government's act was later found to be unconstitutional.[20] Justice Bradley, writing for the majority, found that the

> invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense . . . any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment.[21]

To Justice Bradley, the essence of a search was not merely rummaging through homes and drawers but also "the invasion of his indefeasible right of personal security . . . ."[22] With this characterization, Justice Bradley opened the Fourth Amendment to another possibility—that searches can take place without physical trespass—and redefined the "very essence of constitutional liberty and security."[23]

However, forty years after the groundbreaking decision in *Boyd*, the Court switched back to its old common-law trespass interpretation in *Olmstead v. United States*.[24] Olmstead was the leading conspirator of a criminal enterprise.[25] The government wiretapped his office phone by inserting a small wire along the telephone wires.[26] Notably, the insertion of the small wire did not trespass upon Olmstead's office, but rather were "made in the basement of the large office building."[27] The insertion of this wire became the determining factor of whether the government violated the Fourth Amendment. The Court held that

> one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and message while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation . . . . We think, therefore, that the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.[28]

With that, the Court once again linked the Fourth Amendment to the common-law trespass theory: The Fourth Amendment's protection did not

19. *See id.* at 638.
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.* at 630.
24. *See* Olmstead v. United States, 277 U.S. 438 (1928).
25. *See id.* at 456.
26. *See id.* at 456–57.
27. *Id.* at 457.
28. *Id.* at 466.

reach beyond private territory, and as long as the government did not invade ones individual's house or property, a warrant was not required.

This remained the leading interpretation of the Fourth Amendment from 1928 to 1967. Then *Katz* came along and changed the world.

B. *KATZ*'S NEW FRONTIER: THE REASONABLE EXPECTATION OF PRIVACY

Katz was a landmark Fourth Amendment case for many reasons. The most prominent is that it opened the Fourth Amendment horizon to a world of possibilities beyond physical trespass.

Katz was convicted of transmitting wagering information by telephone across the state lines.[29] The FBI monitored and recorded Katz's phone conversation by attaching a "listening and recording device" outside of a public telephone booth where Katz placed his calls.[30] Because the *public* telephone booth was, arguably, not a private space, the question presented to the Court was "[w]hether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution."[31] The Court called the formation of this issue "misleading" and disagreed on two grounds: first, "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area,' " and second, "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' "[32]

For the first time in nearly forty years, the Court shifted the attention of the Fourth Amendment from "places" to "people."[33] A person can be in his own house or office or a "constitutionally protected area" but not entitled to Fourth Amendment protections for what he "knowingly exposes to the public."[34] On the flip side, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[35] Essentially, the government could trigger Fourth Amendment issues without any physical impingement of individuals' private spaces.[36]

The most impactful part of *Katz* came from Justice Harlan's concurrence, where he stated that "a person has a constitutionally protected *reasonable expectation of privacy* . . . ."[37] This concept of "reasonable expectation of privacy"

29. Katz v. United States, 389 U.S. 347, 348 (1967).
30. *Id.*
31. *Id.* at 350.
32. *Id.*
33. *Id.* at 351.
34. *Id.*
35. *Id.*
36. *See id.* at 350.
37. *Id.* at 360 (emphasis added).

has become a cornerstone of the modern definition of searches. Since *Katz*, a Fourth Amendment search no longer requires an "invasion of a constitutionally protected *area*"—an intrusion upon an individual's reasonable expectation of privacy is sufficient to trigger the plethora of protections under the Fourth Amendment.[38]

C. THE BIRTH OF THE THIRD-PARTY DOCTRINE

Not long after lifting the physical intrusion requirement, the Court created a carve-out rule under Fourth Amendment search—the third-party doctrine. Two cases marked the beginning of this new era—*United States v. Miller* and *Smith v. Maryland*.

In *Miller*, the government subpoenaed copies of Miller's check and bank records to prove that Miller committed tax fraud.[39] The subpoenaed records "had been maintained by the banks in compliance with the requirements of the Bank Secrecy Act of 1970, 84 Stat. 1114, 12 U.S.C. § 1829b(d)."[40] Miller moved to suppress these records at trial on Fourth Amendment grounds, arguing that these records were the fruit of an unreasonable search and seizure. However, the Court found no protectable Fourth Amendment interest in the subpoenaed documents.[41] The Court held that the documents at issue were not subject to the Fourth Amendment protection as it "perceived no legitimate 'expectation of privacy' in their contents."[42] Specifically, the Court found "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[43] Furthermore, the Court held that demanding records from a third party did not violate the rights of the defendant, because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."[44]

Three years after *Miller*, the Court refined the third-party doctrine in *Smith v. Maryland*.[45] In *Smith*, the police requested that the phone company install a

38. *Id.* at 361.
39. *See* United States v. Miller, 425 U.S. 435, 437 (1976).
40. *Id.*
41. *See id.*
42. *Id.* at 442.
43. *Id.*
44. *Id.* at 443.
45. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

pen register[46] to record the numbers that Smith, a robbery suspect, dialed from his home phone.[47] The register later revealed that Smith had called a robbery victim.[48] Based on this evidence, the police arrested Smith, who was identified by the victim as the man who had robbed her.[49] Smith was soon indicted.[50]

Smith sought to suppress the phone number recorded by the pen register on pretrial motions on the ground that the police "had failed to secure a warrant prior to its installation."[51] The Court, however, rejected that argument on two grounds. First, the Court questioned whether

> [p]eople in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company . . . . All subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial . . . .[52]

Though the Court acknowledged that Smith might hold some subjective expectations of privacy which "cannot be scientifically gauged," it was hard to "believe that phone subscribers . . . harbor any general expectation that the numbers they dial will remain secret."[53]

Second, the Court reasoned that "even if [Smith] did harbor some subjective expectation . . . this expectation is not 'one that society is prepared to recognize as reasonable.' "[54] These two reasons led to the conclusion that Smith

> can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed.[55]

Consequently, the Court held that "the installation and use of a pen register . . . was not a 'search,' and no warrant was required."[56]

---

46. 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) (2012).

47. *See id.*

48. *See id.*

49. *See id.*

50. *See id.*

51. *Id.*

52. *Id.* at 742.

53. *Id.* at 743.

54. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

55. *Id.* at 744.

56. *Id.* at 745–46.

With that, the third-party doctrine was solidified. When an individual voluntarily reveals information to a third party, the individual harbors no reasonable expectation of privacy in that information.[57] *Miller* and *Smith* marked the beginning of the third-party doctrine, and at that stage, no limit was placed on this doctrine—it could arguably govern any type of information voluntarily disclosed to third parties, regardless of the nature of the information. Throughout the years, the Court has not had a chance to confront this question or address its scope. Thus, its applicability was always presumed unless clearly prohibited by the Court.

Until *Carpenter*.

III. CASE SUMMARY & REACTIONS

A. FACTUAL BACKGROUND

In April 2011, four men were arrested for a series of robberies of Radio Shack and T-Mobile stores. One of them confessed and gave the FBI a list of fifteen others who had participated in the robbery.[58] Pursuant to the Stored Communication Act, but without obtaining a warrant, the FBI obtained an order from a magistrate judge and demanded from MetroPCS and Sprint the "transactional record" from sixteen phone numbers, including Carpenter's. The record included the "cell-site information for the target telephones at call origination and at call termination for incoming and outgoing calls."[59] The government used this record to show that Carpenter was in the vicinity of the stores at the time of the robberies, and he was charged with six counts of robbery.[60]

B. PROCEDURAL HISTORY

Prior to trial, Carpenter sought to suppress the cell-site location information evidence, arguing its acquisition by the government was a warrantless Fourth Amendment search.[61] The district court denied the motion, and Carpenter was convicted on all counts of robbery and was sentenced to more than one hundred years in prison.[62]

On appeal to the Sixth Circuit, Carpenter argued that the government's acquisition of the cell-site location information was an unreasonable search because the government did not have a warrant supported by probable cause.[63] The Sixth Circuit relied on the third-party doctrine from *Miller* and *Smith* and

57. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976); *Smith*, 442 U.S. at 745–46.
58. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
59. *Id.*
60. *Id.*
61. *Id.*
62. *See id.* at 2213.
63. *See id.*

held that the government did not violate the Fourth Amendment because Carpenter "lacked a reasonable expectation of privacy in the location information . . . [because he] voluntarily convey[ed] cell-site data to . . . [his] carrier[ ] as 'a means of establishing communication.' "[64] The Supreme Court granted certiorari on the Fourth Amendment issue.[65]

C. MAJORITY OPINION

The majority began with a discussion of what the Fourth Amendment protects in the digital age as advancements in technology greatly enhanced the government's surveillance power.[66] Acknowledging the Fourth Amendment's historical tie to physical intrusions, Chief Justice Roberts pointed out that even in the pre-*Katz* era, the Fourth Amendment not only protected property interests, but also "seeks to secure 'the privacies of life' against 'arbitrary power.' "[67] Other precedents provided that the Fourth Amendment was aimed at "[placing] obstacles in the way of a too permeating police surveillance."[68] With these foundations in mind, the Court proceeded to discuess how the Court has traditionally applied the Fourth Amendment to technological innovations in surveillance tools.

Technological advancements have greatly empowered government surveillance tools to "encroach upon areas normally guarded from inquisitive eyes . . . ." [69] Because technology greatly enhanced the government's surveillance capacity, Chief Justice Roberts suggested the Court should "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[70] The Court then used *Kyllo* and *Riley* as examples of how the Court had applied the above principles when deciding cases that involved technological advancements in surveillance tools.[71]

The Court then moved on to apply the Fourth Amendment understandings to Carpenter's case. The Court first acknowledged that, although cell-site location information is data maintained by a third-party, this

64. *Id.*
65. *See id.*
66. *See id.* at 2214.
67. Boyd v. United States, 116 U.S. 616, 630 (1886).
68. *Carpenter*, 138 S. Ct. at 2214 (citing United States v. Di Re, 332 U.S. 581, 595 (1948)).
69. *Id.*
70. *Id.*
71. *See id.* (the Supreme Court held that the government's warrantless search was unconstitutional in both *Kyllo* and *Riley*. Both involved advanced technologies that the government used as surveillance tools. In *Kyllo*, the Court found the government's usage of a thermal detector without a warrant a violation of the Fourth Amendment because the technology could "leave homeowners 'at the mercy of advancing technology . . . .' " Likewise in *Riley*, the Court required the government to obtain a warrant before searching the content of a phone because of its "immense storage capacity").

particular information does not fit squarely under existing precedent.[72] Rather, it lies at the intersection of two lines of cases: one that "addresses a person's expectation of privacy in his physical location and movements," and the one that addresses "what a person keeps to himself and what he shares with others."[73] In the first line of cases, the Court distinguished *Knotts*, a case involving a tracking beeper, from *Jones*, a case involving GPS.[74] The Court distinguished the amount of surveillance implicated in *Knotts* and *Jones*. The GPS in *Jones* was a more sophisticated form of tracking device than the beeper in *Knotts*, because it tracked and monitored "every movement" of a vehicle.[75] The Court agreed with concurring Justices in *Jones* in that " 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large."[76]

In the second line of cases, the Court distinguished between "what a person keeps to himself and what he shares with others."[77] According to the Court's decision in *Miller* and *Smith*, a person could not have a legitimate expectation of privacy if that person voluntarily shared information with a third-party. A strict application of the rule would mean the government could not have triggered any Fourth Amendment issues when it demanded the voluntarily disclosed information from third-parties.[78]

However, the Court declined to apply *Miller* and *Smith* in *Carpenter*.[79] As the Court recognized, the phenomenon presented in *Carpenter* was a "qualitatively different category" from those in *Miller* and *Smith*.[80] The technology in *Carpenter* had "the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring [the court] considered in *Jones*."[81] Thus, as in *Jones*, "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]," and "[a]llowing government access to cell-site records contravenes that expectation."[82]

72. *See id.*
73. *Id.* at 2215, 2216.
74. *See id.* at 2215.
75. *Id.*
76. *Id.*
77. *Id.* at 2216.
78. *Id.*
79. *Id.* at 2217.
80. *Id.* at 2216.
81. *Id.*
82. *Id.* at 2217.

The fact that cell-site location information required a cell phone triggered greater concern for the Court.[83] As it had previously noted in *Riley*, the feature that made a cell phone stand out was that

> [u]nlike the bugged container in *Knotts* or the car in *Jones*, a cell-phone—almost a 'feature of human anatomy,'—tracks nearly exactly the movements of its owner . . . [it] faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . . Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.[84]

In addition to the intrusiveness of cell phones, the Court also found the quality of the cell-site location data critical, as they opened the door for the government to "a category of information otherwise unknowable."[85] Because cell-cite location information is continuously being recorded by phone carrier companies for each and every device in the United States—that is, nearly 400 million devices—the capacity of this information is daunting. The government could easily obtain, without passing the hurdle of the Fourth Amendment, an individual's whereabouts for the past five years.[86]

The Government disputed the accuracy of the cell-site location data, contending that cell-site location was less precise than GPS.[87] Nevertheless, the Court refused to entertain that argument.[88] The accuracy only reflected the current state of the technology, the Court reasoned, and new technology would be able to pinpoint location, just like GPS.[89] Wary of the capacity of the rapidly developing surveillance technology, the Court determined that "[a]t any rate, the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.' "[90] With that, the Court concluded that accessing cell-site location information "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movement."[91]

The Government's next contention was that the case should be governed by the third-party doctrine as "cell-site records . . . are 'business records' created and maintained by the wireless carriers."[92] However, the Court pointed out that the Government failed to take into account the "seismic shifts in

83. *See id.* at 2218.
84. *Id.*
85. *Id.*
86. *Id.*
87. *See id.*
88. *See id.*
89. *See id.* at 2219.
90. *Id.* at 2218.
91. *Id.* at 2219.
92. *Id.*

digital technology."[93] It has been decades since *Smith* and *Miller*, and there has been "a world of difference" between the technology then and now.[94] This case turned on "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[95] Such a chronicle, the Court held, "implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[96]

Next, the Court considered whether cell-site location information fits squarely within the "voluntary exposure" rationale of the third-party doctrine.[97] The Court found that it did not.[98] First, the location information was not truly voluntarily "shared" because cell phones were a "pervasive and insistent part of daily life" and not using one to avoid exposing location information to cell towers is not a realistic option in this era.[99] Second, "[v]irtually any activity on the phone, without any affirmative act on the part of the user beyond powering up," could generate cell-site location data.[100] It was therefore impossible not to share that information unless the phone was off.[101] Thus, the Court concluded that "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."[102] The Court subsequently declined to extend the third-party doctrine to this case and held that "[t]he government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."[103]

This decision was, in the Court's own words, "a narrow one"—the Court did not venture to decide how this decision would apply to other modern digital technologies.[104]

D. DISSENTING OPINIONS

Carpenter was a 5–4 decision with each dissenting Justice filing a separate opinion. While the dissenting Justices all wrote extensively, in the interest of time, this Section summarizes their main standpoints from a high level.

Their main arguments against the majority were 1) the historical interpretation of the Fourth Amendment has always been tied to personal

93. *Id.*
94. *Id.*
95. *Id.* at 2220.
96. *Id.*
97. *Id.*
98. *See id.*
99. *Id.*
100. *Id.*
101. *See id.*
102. *Id.*
103. *Id.*
104. *Id.*

property; 2) the third-party doctrine should apply to cell-site location information; and 3) the compulsory process was an important investigative tool for the government to solve crimes. Justice Gorsuch's dissent suggested three potential frameworks that could be used in analyzing data privacy cases: 1) apply *Smith* and *Miller* and live with the consequences; 2) go back to *Katz*'s reasonable expectation of privacy test; and 3) look for an answer elsewhere.[105] Throughout his dissent, Justice Gorsuch expressed his resentment towards *Katz*'s reasonable expectation of privacy and the third-party doctrine. He disagreed "with the Court's decision [] to keep *Smith* and *Miller* on life support, supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared."[106]

E. COMMENTATORS & LOWER COURT REACTIONS

Carpenter is a relatively new decision, and there are only a handful of law review articles[107] and a draft of two chapters of a book dedicated to *Carpenter* and its impact.[108] Most comments and reactions exist in multiple online forums and blogs.

Notably, the reputable Fourth Amendment scholar, Orin Kerr, who filed an amicus brief on behalf of the United States, suggested that this case falls squarely within his "equilibrium-adjustment" theory.[109] The equilibrium-adjustment theory suggests that "when new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[110] What this means is that if a new technology grants power to the government that could lead to potential abuse based on old rules, the Court will "expand[] legal protection to restore old levels of power and limit abuses."[111] By the same token, if a technology that narrows the power of the government would "unduly limit the government's ability to solve crimes under old rules," the Court will restrict the scope of the legal protection "to restore old levels of power and ensure the government can still solve enough cases."[112] *Carpenter*,

105. *See id.* at 2262.

106. *Id.* at 2272.

107. *See, e.g.*, Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205 (2018).

108. *See* Orin S. Kerr, *Implementing Carpenter* (USC Law Legal Studies Working Paper No. 18-29, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/4KLR-Z2GV].

109. *See* Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/6B7N-4TWL].

110. Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

111. Kerr, *supra* note 109.

112. *Id.*

as Orin Kerr saw it, was the Court expanding Fourth Amendment protection to prevent the government from abusing its power using advanced surveillance technology.

Professors Freiwald and Smith saw this decision as the Court "confront[ing] the challenges of twenty-first-century technology."[113] They suggested that the Court adopt a multifactor analysis, including whether the cell-site location information is hidden, continuous, indiscriminate, or intrusive and its expense and efficiency to determine "whether CSLI acquisition is a search under the Fourth Amendment."[114] The Article criticized the third-party doctrine as being a framework "rest[ing] on a shaky foundation."[115] Acknowledging that the majority's decision was a narrow one, Professors Freiwald and Smith argued that "the scope and rationale of the opinion send clear signals for certain other location monitoring techniques" and "provides a useful framework for courts to evaluate Fourth Amendment limits on the state's access to digital database . . . ."[116] Towards the end of the Article, they lamented the "extraordinary length of time" it took the Court to "reach a definitive answer on how the Constitution applies to the data continuously emitted by the signature device of our era—the cell phone."[117] Lastly, they called for a better system of policing the constitutional constraints on law enforcement's conducts in the face of their powerful new surveillance tools.[118]

Other comments from online forums about *Carpenter* are polarized as the commentators disagree over the applicability and the precedential value of *Carpenter*.[119] Some criticized the Court for wasting too much time on reasonable expectations of privacy and the third-party doctrine while overlooking the fact that the problem can be solved easily by the heart of the Fourth Amendment—it "protects people, not places."[120] Several applauded

113. Freiwald & Smith, *supra* note 107, at 206.

114. *See id.* at 220–21.

115. *Id.* at 225.

116. *Id.* at 227.

117. *Id.* at 227, 231.

118. *Id.* at 234–35.

119. *See* Paul Rosenzweig, *Carpenter v. United States and the Law of the Chancellor's Foot*, LAWFARE (June 27, 2018), https://www.lawfareblog.com/carpenter-v-united-states-and-law-chancellors-foot [https://perma.cc/M7LV-UY3D] (criticizing the Court's opinion being too narrow and its lack of predictability).

120. Mike Godwin, *What's Next for the Reasonable Expectation of Privacy? The Supreme Court's Ruling in* Carpenter *Raises New Questions*, SLATE (June 27, 2018), https://slate.com/technology/2018/06/after-the-supreme-courts-carpenter-ruling-where-is-the-reasonable-expectation-of-privacy-heading.html [https://perma.cc/QTH7-Y3UW] (arguing that the main issue in *Carpenter* was not the record, but rather, "when your phone company gathers location information about your phone . . . they're searching (or in some sense, seizing) *you*").

Justice Gorsuch's dissent for openly criticizing the third-party doctrine.[121] Some even went as far to say that "[u]ltimately, the future of Fourth Amendment jurisprudence may be in the hands of Justice Gorsuch, who has clearly indicated that the third-party doctrine . . . needs to be discarded."[122]

However, these reactions failed to capture the essence of the *Carpenter* holding. The equilibrium-adjustment theory, while seemingly predicting outcomes correctly, can explain almost everything in hindsight. This theory tries to broadly hew the Court's decisions to the notion of "equilibrium," whose very definition is indeterminant. Had Carpenter come out the other way, this theory would also be the perfect vehicle to explain its reasoning—it could be easily argued that a warrant is not required because it leaves law enforcement with too little power to solve crimes. The theory suggests that there will be, at some point, some form of pushback on government power if it goes too far. It requires the assessment of how much power is too much. However, that assessment is subjective, and it is impossible to know where that line lies until the Court reaches a decision. When the same theory can justify opposing outcomes, it is not a helpful guide for the Justices.

As for whether the fate of the third-party doctrine ultimately lies in the hands of Justice Gorsuch, it is too early to tell. The five Justices in the majority opinion are still sitting on the bench, while Justice Kennedy has retired. Although Justice Kavanaugh has authored several opinions in which he "consistently favored law enforcement and government surveillance over the privacy of individuals,"[123] it is unclear whether he will follow Justice Kennedy's path. With the current composition of the Court, it is unlikely that Justice Gorsuch could single-handedly change the landscape of the third-party

121. *See id.* ("Justice Neil Gorsuch's dissent is . . . in some ways . . . the best of the dissents [as he] is looking toward the future as well as the precedential past."); *see also* Taylor Millard, *Justice Gorsuch's Fascinating, Constitutional Dissent in Carpenter*, HOT AIR (June 24, 2018), https://hotair.com/archives/2018/06/24/justice-gorsuchs-fascinating-constitutional-dissent-carpenter/ [https://perma.cc/4RNW-68YQ] ("[Gorsuch's] arguments are beyond sound and something which is sorely missing in American legal theory.").

122. Ashley Baker, *Gorsuch's Dissent in 'Carpenter' Case Has Implications for the Future of Privacy*, HILL (June 26, 2018), https://thehill.com/opinion/cybersecurity/394215-gorsuchs-dissent-in-carpenter-case-has-implications-for-the-future-of [https://perma.cc/B6J8-SW96].

123. Elec. Privacy Info. Ctr., *Brett M. Kavanaugh and Privacy*, EPIC.ORG, https://epic.org/privacy/kavanaugh/ [https://perma.cc/W6T6-M2KD] (last visited Dec. 17, 2018); *see, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1 (2013) (defending post-9-11 surveillance of the American public on third-party doctrine and national security grounds); United States v. Maynard, 615 F.3d 544 (2010), *aff'd*, 565 U.S. 400 (2012) (Kavanaugh, J., dissenting) (finding that the law enforcement officer's "unauthorized physical encroachment within a constitutionally protected area" a more important issue than the tracking power of GPS); United States v. Askew, 529 F.3d 1119 (2008) (Kavanaugh, J., dissenting) (finding that it was reasonable for a police officer to unzip a suspected armed robber's jacket).

doctrine. Nevertheless, nothing can be said with any level of certainty, as it is unlikely that the Court will hear another privacy case for a while.

Since the ruling came down in June 2018, courts have only had a handful of opportunities to grapple with the *Carpenter* decision and apply it to other types of data, including utility records,[124] IP addresses,[125] and real-time location information.[126] However, almost six months later, courts have yet to extend *Carpenter* to location information beyond cell-site location information.[127] This outcome is not in conflict with *Carpenter*, though, as none of the above types of data generate any exhaustive record that chronicles an individual's physical location over many years like cell-site location information.

These arguments do have their merits, but commentators failed to recognize that *Carpenter* was not a groundbreaking decision. Commentators have overlooked the consistent pattern that the Court has followed when treating cases involving technological advancements. *Carpenter* was, in effect, an extension of a course that the Supreme Court has charted since the beginning of the century.[128]

IV. ANALYSIS & APPLICATION

Carpenter ultimately came down to a 5–4 decision, with the majority upholding the privacies of life that the Fourth Amendment seeks to protect. Despite the numerous interpretations and theories offered by commentators, district and circuit court judges will eventually have to go back to the majority opinion to determine what is and is not protected by the Fourth Amendment. This Part of the Note interprets the majority's opinion, its implications, its

124. *See* United States v. Chad Lightfoot, No. CR 17-0274, 2018 WL 4376509, at *6 (W.D. La. Aug. 30, 2018) (holding that *Carpenter* does not extend to "information retained by other service related industries, including utility records").

125. *See, e.g.*, United States v. Contreras, No. 17-11271, 2018 WL 4689962 (5th Cir. Oct. 1, 2018) (finding that residence information obtained through IP addresses "falls comfortably within the scope of the third-party doctrine"); Cryer v. Idaho Dep't of Labor, No. 1:16-CV-00526-BLW, 2018 WL 3636529 (D. Idaho July 30, 2018); United States v. Monroe, No. CR 16-00055 WES, 2018 WL 5717367 (D.R.I. Nov. 1, 2018); United States v. Rosenow, No. 17CR3430 WQH, 2018 WL 6064949, at *11 (S.D. Cal. Nov. 20, 2018).

126. *See, e.g.*, Andres v. State, No. SC15-1095, 2018 WL 4496567 (Fla. Sept. 20, 2018) (finding that *Carpenter* does not extend to "real-time cell-site location information to locate [the defendant] for the purposes of executing the warrant"); United States v. Hammond, No. 3:18-CR-5 RLM-MGG, 2018 WL 5292223 (N.D. Ind. Oct. 24, 2018) (denying defendant's motion to suppress government's use of real-time location under the good-faith exception).

127. *See* People v. Simpson, No. 01027-2017, 2018 WL 6210585, at *2 (N.Y. Sup. Ct. Sept. 4, 2018) (extending *Carpenter* to collection of three days of cell-site location data and holding that "[t]he distinction between the seven days of CSLI in the *Carpenter* decision and the three days of CSLI in the instant case is de minimis").

128. *See infra* Part IV.

impact on the third-party doctrine and the reasonable expectation of privacy, and the extent of the Fourth Amendment's protection in the digital age.

A. THE "PRIVACIES OF LIFE" IN THE DIGITAL ERA & THE ROAD TO *CARPENTER*

Some Fourth Amendment scholars, like the dissenting Justices, thought that *Carpenter* strayed too far from the historical property-based understanding of privacy. To the contrary, the Court has long been devoted to protecting individual's information privacy in the face of seismic shifts in technology. The next Section examines the reasoning and the outcomes of three pre-*Carpenter* privacy cases, *Kyllo*, *Jones*, and *Riley*, and how these cases paved a clear path that eventually led to *Carpenter*.

1. Kyllo

Kyllo v. United States[129] was one of the first cases that dealt with the government's use of advanced technology and the parameters of Fourth Amendment protection. In *Kyllo*, an agent was suspicious that Kyllo was growing marijuana in his home.[130] Knowing that growing marijuana indoors requires high-intensity lamps, the agent scanned Kyllo's house using a thermal imager to detect the amount of heat emitting from the house.[131] The scan showed that the roof over the garage was hotter compared to other rooms of the house, which made the agent conclude that Kyllo was using high-intensity lamps in his house to grow marijuana.[132] Based on this evidence, the agent obtained a warrant, searched Kyllo's home, seized the marijuana, and indicted him.[133] Kyllo moved to suppress the evidence from the thermal imager but was unsuccessful.[134]

In rejecting Kyllo's challenge, the district court found that the thermal imager was not intrusive as it "emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house . . . [it] 'cannot penetrate walls or windows to reveal conversations or human activities' . . . and 'no intimate details of the home were observed.' "[135] The Supreme Court disagreed. Justice Scalia wrote for the Court and first reinforced that " '[a]t the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusions.' "[136] Second, Justice Scalia backed Justice Harlan's concurrence in

129. 533 U.S. 27 (2001).
130. *Id.* at 29.
131. *Id.*
132. *Id.* at 30.
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.* at 31 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

Katz that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[137] Turning to the facts in *Kyllo*, Justice Scalia concluded that using a thermal imager constituted a Fourth Amendment search, as the government obtained information that they could not have obtained "without physical 'intrusion into a constitutionally protected area.' "[138] Thus, information collected from the thermal imager was the fruit of a search.

Fearing that the rapid development of technology might "leave the homeowner at the mercy of advancing technology," the Court felt it necessary to adopt a rule that "take[s] account of more sophisticated systems that are already in use or in development."[139] With that, the Court announced its direction going forward, which was to protect individuals' privacies of life from the government's exploitative use of sophisticated technology.

2. Jones

Jones followed the steps of *Kyllo*.

To understand the significance of *Jones*, one must first take note of a preceding case: *United States v. Knotts*.[140] *Knotts* was decided in 1983, a time when the technology of tracking devices was still rudimentary. In *Knotts*, law enforcement agents placed a beeper on a chloroform container that was loaded onto a vehicle in order to monitor and trace it.[141] The agents followed signals given off by the beeper and traced the chloroform container from Minnesota, where it was purchased, to Knott's secluded cabin in Wisconsin.[142] With this evidence, the law enforcement agents arrested Knotts for conspiring to manufacture controlled substances.[143] Knotts objected to the beeper recordings on the ground that it was a warrantless search.[144] The Court disagreed.[145] It held that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movement from one place to another."[146] Beepers, as the Court pointed out, "are merely a more effective means of observing what is already public."[147] Thus, the Court held that the government's act did not violate the Fourth Amendment.

137. *Id.* at 33 (citing Katz v. United States, 389 U.S. 347, 361 (1967)).
138. *Id.* at 34.
139. *Id.* at 35–36.
140. 460 U.S. 276 (1983).
141. *See id.* at 277.
142. *See id.*
143. *See id.* at 279.
144. *See id.*
145. *See id.* at 280.
146. *Id.* at 281.
147. *Id.* at 285.

What the Court did not anticipate in 1983 was the rapid development of tracking devices—GPS quickly became prevalent and ubiquitous by 2012. That was when *Jones* came before the Court, prompting it to reconsider the capacity of tracking devices.[148]

Jones was the suspect of drug trafficking and was being investigated by the FBI.[149] The FBI employed several techniques, including

> install[ing] a GPS tracking device on the undercarriage of the Jeep . . . . Over the next 28 days, the Government used the device to track the vehicle's movements, and . . . [b]y means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and . . . relayed more than 2,000 pages of data over the 4-week period.[150]

With these records, the government obtained a multiple-count indictment against Jones.

The case made its way to the Supreme Court where the Court held that the "installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle movements, constituted a 'search.' "[151] In particular, Justice Sotomayor's concurrence pointed out that "long term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[152] Though both involved tracking devices, *Jones* differed from *Knotts* in that, unlike the beeper, "GPS monitoring 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 . . . [and] [t]he government can store such records and efficiently mine them for information years into the future."[153] Justice Sotomayor also emphasized the advancement of GPS tracking technology compared to other forms of tracking techniques, in that "GPS monitoring is cheap in comparison to the conventional surveillance techniques, and by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.' "[154] Applying the reasonable expectation test in *Katz*, it seemed obvious whether "people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[155] GPS can be easily abused by law

148. United States v. Jones, 565 U.S. 400 (2012).
149. *See id.* at 402.
150. *Id.* at 403.
151. *Id.* at 404.
152. *Id.* at 415.
153. *Id.*
154. *Id.* at 415–16.
155. *Id.* at 416.

enforcement to chronically track individuals in their private spaces and, without any oversights, can lead to "a too permeating police surveillance."[156] Thus, the Court held that GPS monitoring was a search.[157]

3. Riley

Fast forward to the age of Apple, Android, and Samsung: *Riley v. California*,[158] decided in 2014, involved an even more powerful technology—cell phones.[159]

Riley was pulled over by a police officer for driving with an expired registration.[160] Over the course of this stop, the police officer discovered that Riley was in possession of a concealed and loaded gun.[161] He was arrested and his cell phone was seized and its contents reviewed.[162] A detective who had "fully examined the contents of the cell phone" testified that the content in the phone confirmed that Riley was a gang member.[163] Riley was charged based on this evidence.[164] He moved to suppress the evidence the police obtained from his phone on Fourth Amendment grounds.[165]

The Court agreed with Riley and concluded that "the fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely."[166] Especially with regard to cell phones, the Court expressed its grave concern that they, "as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[167] The feature that distinguished cell phones from the rest of these items was their vast capacity:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, videos players, rolodexes, calendars, tape recorders, libraries, albums, televisions, maps or newspapers.[168]

156. *Id.* at 416–17 (citing United States v. Di Re, 332 U.S. 581, 595 (1948)).
157. *Id.* at 402.
158. 134 S. Ct. 2473 (2014).
159. *See generally id.*
160. *See id.* at 2480.
161. *See id.*
162. *See id.*
163. *Id.* at 2480–81.
164. *Id.* at 2481.
165. *Id.*
166. *Id.* at 2488.
167. *Id.* at 2488–89.
168. *Id.* at 2489.

What is even more notable is their "immense storage capacity."[169] Most people cannot carry with them the physical copy of every piece of mail they have received over the course of several years, the books and articles that they have read, the pictures and videos they have taken, the webpages they have visited—"nor would they have any reason to attempt to do so."[170] However, one can easily do so by carrying a current top-selling cell phone, as they have the capacity to store enough information to "construct a virtual clone of that individual."[171]

The Court went on to discuss what it meant to have such a vast storage capacity and its impact on privacy. First, the Court found that a phone was an all-in-one device for an "address book, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."[172] Second, even if a phone had just one feature, its capacity "allows even just one type of information to convey far more than previously possible."[173] Just take photos for example, where "an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and description."[174] Third, the phone records data can be traced back to months or even years.[175] As the Justices pointed out, "[a] person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past seven months, as would routinely be kept on a phone."[176]

Finally, the Court addressed the sensitivity of cell phone records.[177] Prior to having phones, people "did not typically carry a cache of sensitive personal information with them as they went about their day."[178] But we are in a different world—nearly 75% of cell phone users stay within five feet of their phones most of the time. Some even use phones in their shower.[179] "Today . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from mundane to the intimate."[180]

---

169. *Id.*
170. *Id.*
171. Aaron Brown, *This Is How Much YOUR Smartphone Knows About You Right NOW*, EXPRESS (May 7, 2016), https://www.express.co.uk/life-style/science-technology/667868/Smartphone-Knows-About-You-Tracking [https://perma.cc/M2ZD-5MUZ].
172. *Riley*, 134 S. Ct. at 2489.
173. *Id.*
174. *Id.*
175. *See id.*
176. *Id.*
177. *See id.* at 2490.
178. *Id.*
179. *See id.*
180. *Id.*

Cell phone records' intrusiveness goes beyond the amount of information they can store. Some of the stored information is qualitatively different from physical records. For example, internet searches can reveal an individual's private interests; application software can reveal an individual's political interest, intimate, financial, and other sensitive information.[181] The truth is, cell phones are not just advanced technological devices. What they are capable of storing, and the sensitive nature of the information they store are what many Americans call "the privacies of life."[182] The fact that this technology came along in the twenty-first century "does not make the information any less worthy of the protection for which the Founders fought" in the eighteenth century.[183] With that, the Court held that the government may not search a cell phone without a warrant supported by probable cause.[184]

4. The Road to Carpenter

A closer read of the precedent reveals that the Court has always been wary of sacrificing individual's "privacies of life" to the government's dazzling new gadgets. The Court had long recognized the power of technology and had been extending the scope of Fourth Amendment protection every time the government's sophisticated technology posed new threats to individual's privacy. Throughout the years, the Court had been consistent in that position. It was consistent in *Kyllo*, *Jones*, and *Riley*, and it was consistent in *Carpenter*.

Starting from *Kyllo*, the Court disallowed the use of technology that could circumvent "physical intrusion" on an individual's home.[185] The Court recognized that using a sense-enhancing thermal imager to detect heat radiation from a house allows the government to easily know everything inside the house without physically raiding it. Using a surveillance device like this to "explore details of the home that would previously have been unknown without physical intrusion . . . is a 'search' and is presumptively unreasonable without a warrant."[186] The Court departed from the mechanical interpretation of the Fourth Amendment so as not to "leave the homeowner at the mercy of advancing technology."[187] This departure from the historical interpretation of the Fourth Amendment set the first stone towards the Court's long battle against advanced technologies that impinge on personal privacies.

The Court continued to pave the way in *Jones*. Comparing GPS technology with the bumper beeper in *Knotts*, the Court recognized that GPS was much more sophisticated—it could generate a wealth of "precise, comprehensive

181. *See id.*
182. *Id.* at 2494–95.
183. *Id.* at 2495.
184. *See id.*
185. Kyllo v. United States, 533 U.S. 27, 40 (2001).
186. *Id.*
187. *Id.* at 35.

record[s]" of a person's movements.[188] The individual being tracked by a GPS would have no place to hide.[189] Concerned about the intrusive and revealing nature of GPS, the Court ultimately held that using GPS to track an individual's location was a search.[190] The Court, again, did not sacrifice personal privacy in the face of advancing technology.

Later in *Riley*, the Court followed the same path when it came to cell phones. Cell phones had a vast capacity to store sensitive information that was both qualitatively and quantitatively different from what the Court had previously seen.[191] Allowing the government to search one's cell phone is to expose one's life to the mercy of the government, because a cell phone can store enough data to reconstruct the user's life.[192] Facing such a powerful, advanced technology, the Court, again, chose to protect the privacies of life—as it had done in *Kyllo* and *Jones*.

From *Kyllo* to *Jones* to *Riley*, the Court had been sending a clear and consistent message. Whenever a "seismic shift" in technology produced information that was qualitatively and quantitatively different, the Court always protected individuals' privacy rights. Since the first time the Court took notice of the use of "sophisticated technology" in *Kyllo*, the Court announced its course going forward: The Court would not allow advancements in technology to erode individuals' reasonable expectations of privacy.

Thus, *Carpenter*'s outcome is no surprise. Cell-site location information was the fruit of a search using sophisticated digital technologies—ones that were unimaginable in the age of *Smith* and *Miller*. With its capability of tracking one's physical movements for five years, cell-site location information was a detailed record of one's whereabouts.[193] This exhaustive chronicle, with its sensitive, pervasive, and intrusive nature, implicated the Fourth Amendment protection against unreasonable searches and seizures.[194] Consistently following the path set by *Kyllo*, *Jones*, and *Riley*, the Court, unsurprisingly, sided with personal privacy against sophisticated technologies by concluding that obtaining cell-site location information was a search.

5. *The Crossover Between the Use of Advanced Technologies and the Third-Party Doctrine*

Carpenter was a special case in many ways. Most prominently, it was a crossover of both the modern interpretation and the traditional interpretation of the Fourth Amendment. The modern interpretation was, as discussed in the

188. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
189. *See id.*
190. *Id.* at 404.
191. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014).
192. *See id.* at 2489.
193. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
194. *See id.* at 2217.

previous Section, protecting privacy rights in the face of advanced technologies; and the traditional interpretation was the third-party doctrine. Under the modern interpretation, obtaining cell-site location information would be a search. Under the straightforward application of the traditional interpretation, it would not.

However, at least as articulated in *Miller* and *Smith*, there was another crucial component required for the third-party doctrine to apply—the nature of the information sought.[195] As the Court pointed out in *Carpenter*, the check records and the phone numbers being demanded in *Miller* and *Smith*, respectively, were not of a sensitive nature.[196] Rather, they were information that had only "limited capabilities" and were not private.[197] The cell-site location information that the Court confronted in *Carpenter*, on the other hand, was "a new phenomenon" produced by sophisticated technology.[198]

In this clash between the modern and traditional interpretation, the Court chose the former.[199] When confronting a type of information that has such a unique nature as the cell-site location information, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[200]

B. THE FATE OF THE THIRD-PARTY DOCTRINE POST-*CARPENTER*

Despite the *Carpenter* decision being a big win for advocates of personal privacy, it did not gain universal approval and garnered polarized reactions. On one hand, Andrew Ferguson called it "a blockbuster Fourth Amendment case," signaling "a new openness to expand the Fourth Amendment to fit digital criminal investigations."[201] On the other hand, Orin Kerr and Paul Rosenzweig called the majority opinion uncertain and, blatantly, "not law."[202] Most disputes were over the majority's treatment of the third-party doctrine: While there seems to be a consensus that the third-party doctrine has been

195. *See id.* at 2219 ("*Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate expectation of privacy concerning their contents.' ").

196. *See id.*

197. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979)).

198. *Id.* at 2216.

199. *See id.* at 2217.

200. *Id.*

201. Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [https://perma.cc/C99Q-9XV7].

202. Rosenzweig, *supra* note 119.

largely curtailed, to what extent it has been curtailed and how the lower courts should apply this ruling in future cases is still up in the air.[203]

Since the third-party doctrine first came down in the 1970s, it has been considered a categorical rule—i.e., it applies to any type of information voluntarily given to a third party. However, upon a closer examination of the *Carpenter* majority, the Court implied that that was not the case—the third-party doctrine applicability was meant to be limited, depending on the nature of the information.[204]

As Justice Frankfurter instructed in *Northwest Airlines* when considering new technology innovations, "the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.' "[205] To put it in context, *Miller* was decided when people were using cash and check to make purchases, and *Smith* was decided before the idea of portable telephones was even conceived. Digital technology has indisputably undergone a seismic shift throughout the decades since *Miller* and *Smith*. Payment methods and telecommunication gadgets have been revolutionized and a great deal of information can be shared with a third party with a lot less voluntary control. For example, cell-site location information is not a like a nosy neighbor that keeps an eye on you as you come and go. It is a detailed, exhaustive, chronicled record of every single physical location at any point in time for the past several years. Its memory is "nearly infallible."[206] Moreover, there is no way to avoid having such a record unless one switches off the internet connection completely or abandons the cell phone altogether.[207] Taking into account the advancement of new surveillance technologies, the Court concluded:

> There 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. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a *significant extension* of it to a distinct category of information.[208]

The phrase "significant *extension*" here bears special importance. Whereas scholars and courts have assumed that the third-party doctrine covered all data in the hands of third parties, the Court here makes it clear that a "straightforward application" of the third-party doctrine would only address

203. *See, e.g.*, Ferguson, *supra* note 201 ("*Carpenter* signals the end of the third-party doctrine as traditionally understood."); Kerr, *supra* note 109 ("[The third-party doctrine] lives, but there is an equilibrium-adjustment cap on it.").

204. *See Carpenter*, 138 S. Ct. at 2219.

205. *Id.* at 2220 (citing Northwest Airlines, Inc. v. Minn, 322 U.S. 292, 300 (1944)).

206. *Id.* at 2219.

207. *Id.* at 2220.

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

the "limited types of personal information addressed in *Smith* and *Miller*."[209] Anything beyond those "limited types" necessarily requires an *extension*. With that, the Court effectively rejected the traditional view that the third-party doctrine was a categorical rule.

This means that the third-party doctrine is still alive, but its applicability is significantly narrowed. However, for lower courts, this holding can be vague. On one end of the spectrum, the limited-type information in *Miller* and *Smith* requires a straightforward application of the third-party doctrine. On the other end, the exhaustive record of someone's location represented by cell-site data would require a significant extension that the Court is not willing to grant. As for the rest of the spectrum between these two ends, the Court did not give a clear guideline as to when the third-party doctrine applies.

Although there is no bright-line rule to determine under what circumstances the third-party doctrine applies and under what circumstances it does not, the Court provided several factors from precedents for the lower courts to consider, including invasiveness and sensitivity from *Kyllo*, pervasiveness and precision from *Jones*, and volume and exhaustiveness from *Riley*. The fundamental question is how much the information sought intrudes upon the individual's privacies of life.

Professor Orin Kerr, in his upcoming book, dedicated one entire chapter on how the ruling of *Carpenter* can be implemented so as to make it less convoluted and subjective.[210] He proposed three possible tests: the Subjective Approach, the Mosaic Theory, and the Source Rule.[211] The Subjective Approach focuses on when the government learns private, *Carpenter*-like information—i.e., a search is triggered "the moment the government learns a private fact about a person that is among the type *Carpenter* regulates."[212] However, this approach entails a good amount of judgment calling, especially when it comes to *when* the information becomes *too* private. Some information, standing alone, might not be as invasive as seven days of cell-site location information, but could reveal intimate, private details when cumulated together.[213]

209. *Id.*

210. *See* Kerr, *supra* note 108, at 27–28.

211. *See id.*

212. *Id.* at 27.

213. *See id.* at 29. Professor Kerr used several scenarios in his paper to demonstrate the power of information accumulation. "The key lesson is that the invasiveness of information is contingent on what else is known. We find information invasive when it supports a conclusion about a person . . . the sense of invasiveness occurs when learning fact A implies sensitive fact B. But whether A implies B often depends on whether we also know C." *Id.* at 34.

The Mosaic Theory focuses on whether the quantity of information obtained is sufficient to trigger the *Carpenter* safeguard.[214] Under this approach, "a search occurs when an information transfer to the government includes a large quantity of *Carpenter*-protected information."[215] However, this approach also calls for a decent amount of subjectivity, as it requires the courts to draw a line between how much information is not broad and how much is too broad. How much is too much? Carpenter concluded that seven days of cell-site location information is impermissible, but what about two days? What if the government first collected two days of information and then collected another two days of information? Should courts consider the two two-days separately or together?[216] This approach provides more questions than answers and "offers no clarity about how much surveillance is enough to trigger a search."[217]

The Source Rule is a bright-line rule, as it focuses on the source that generates the information.[218] This approach takes out the line-drawing process required by the above two approaches and "asks only whether any information revealed to the government was dependent or relied on use of a technology that *Carpenter* covers."[219] Applying this rule is easy—if a court determines that the information revealed is a product of the seismic shift—an advancement—in technology, then all information produced is protected—"[o]ne datum is just as protected as the entire database. It's all protected."[220] Professor Kerr zealously advocates for the Source Rule.[221] However, while the Source Rule provides clarity, it has some significant drawbacks: it can be both over-inclusive and under-inclusive. The Source Rule provides that any information obtained through a *Carpenter*-protected method, even if only a single data point, is protected as a search.[222] However, this practice is over-inclusive because not every data point generated by a *Carpenter*-protected method is enough to be a search. What made the cell-site location data a search in *Carpenter* was that the hundreds of thousands of data points *collectively* created a chronical of someone's life. But one discrete data point is unlikely to have the same effect.

---

214. *Id.* at 28.

215. *Id.* at 28.

216. *See id.* at 37.

217. *Id.* at 39. Professor Kerr is also against the Mosaic Theory, as this theory asks the judges to "make judgments about time, about numbers of events, and about how much the combination of time and numbers leads to a feeling that a line has been crossed." *Id.* at 38.

218. *See id.* at 28.

219. *Id.* at 28.

220. *Id.* at 40.

221. *See id.* at 42. Professor Kerr considered the Source Rule as being able to "reduce the morass of complex questions raised by *Carpenter* into something more manageable . . . the Source Rule brings the challenge of implementing *Carpenter* from seemingly-impossible to just really-hard." *Id.*

222. *See id.* at 40.

On the flip side, this approach is under-inclusive as it only covers the existing technologies examined by the Supreme Court but not the upcoming new technologies that are being constantly developed and deployed by the government and private sector. Given the speed of technology advancement, sooner or later, the government will have a new gadget, not covered by *Carpenter*, that could trigger Fourth Amendment concerns—how then should the courts decide? The lower courts would then have to go back to the holding of *Carpenter* and seek answers there—i.e., considering various factors and decide how much information is *too much*.

C. THIRD-PARTY DOCTRINE APPLIED TO TECHNOLOGIES IN THE POST-*CARPENTER* ERA

This Section is devoted to discussing how the majority's decision in *Carpenter* could apply to several technological advancements in the post-*Carpenter* digital era, such as cell-site simulators (aka Stingray), voice-command home devices, such as Amazon Echo, and credit card records.

1. Cell-Site Simulator (Stingray)

Cell-site simulators, or more colloquially known as Stingray,[223] are devices that "mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information."[224] Cell-site simulators emit stronger signals than the cell towers nearby and trick cell-phones to disconnect from legitimate cell towers and connect to these simulators.[225] It is difficult, if not impossible, for cell-phone users to know when their phones are connecting to a simulator.[226] Once a device has connected to a simulator, the simulator can track the user's location and read "identifying data directly from [the] mobile device."[227] Advanced simulators can even intercept incoming phone calls and messages and "divert calls and text messages, edit messages, and even spoof the identity of a caller in text messages and calls."[228]

223. *See generally* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012).

224. *Stingray Tracking Devices*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices [https://perma.cc/9XSB-KJDX] (last visited Apr. 9, 2019).

225. *Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/TH5K-AD43] (last visited Apr. 9, 2019) [hereinafter *EFF on Cell-Site Simulators*].

226. *Id.*

227. *Id.*

228. *Id.*

State and local police departments nationwide possess this surveillance technology.[229] Their prevalence is concerning, as not only can cell-site simulators be used to uncover information about a suspect, when they are used to track someone's cell phone, they can also simultaneously gather information "about the phones of countless bystanders who happen to be nearby."[230] Furthermore, cell-site simulators can be used discretely, as some are small enough to fit in a police vehicle and can be driven around to multiple locations, gathering data from every mobile device around those areas—including devices located in traditionally protected areas, such as someone's home.[231]

Given the wide coverage and the capability of cell-site simulators—in some cases one simulator can connect up 10,000 mobile devices at a time[232]—it seems like there is no doubt that location data collected by these simulators deserve Fourth Amendment protection. First of all, cell-site simulators, by their very nature, generate the same type of data as cell towers do. Thus, all the *Carpenter* rationales are applicable here. Second, cell-site simulators have a wider coverage than cell towers because they can travel around in police cruisers. These simulators graze neighborhoods, collect location data from mobile devices in houses, apartments, and private spaces, triggering serious privacy concerns. Third, the data collected by these simulators are indiscriminate. While law enforcement officers might have a warrant to track a suspect's device,[233] cell-site simulators collect much more information than is covered by that warrant, as they could potential collect information from thousands of other non-suspect devices. The breadth of the search "raises the specter of an illegal general warrant."[234] Fourth, cell-site simulators can do more than just passively receiving data—they can also intercept calls and texts and identify the caller. Treading into individual's private communication is no less intrusive than searching someone's cell-phone, as in *Riley*. Lastly, unlike the cell-site location information in *Carpenter*, cell-site simulators are operated by law enforcement officers, and the data are collected by law enforcement officers, not by a third-party provider. Thus, there is no third-party doctrine issue at play that could shield a Fourth Amendment violation. Based on the

229. *Stingray Tracking Devices: Who's Got Them*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/KP9P-JC7A] (last visited Apr. 9, 2019) (noting the ACLU has identified "75 agencies in 27 states that the District of Columbia that own stingrays").

230. *Id.*

231. *Id.*

232. *EFF on Cell-Site Simulators*, *supra* note 225.

233. Since 2016, DOJ requires law enforcement officers to seek a Rule 41 warrant to use cell-site simulators. *See* DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015).

234. Freiwald & Smith, *supra* note 107, at 229.

foregoing, it should be the case that the data collected by cell-site simulators are subject to Fourth Amendment protection.

2. "Alexa, call XXX"

The next technology advancement discussed in this Section is Amazon's home smart speaker, Amazon Echo. Today, nearly sixteen percent of Americans, or around 39 million people, own a smart speaker, including four percent of Google Home users and eleven percent of Amazon Echo users.[235] Amazon Echo and its shorter kin, Echo Dot, were the top sellers in 2017.[236]

Amazon Echo is a comprehensive home electronic artificial intelligence system that performs multiple tasks with verbal commands.[237] Here is how it works: The default name of Echo is "Alexa," which Amazon calls the devices' "wake-up word."[238] Echo will always be listening for the wake up word, and when it hears it, a ring of blue LED light will light up, indicating that Echo is starting to record.[239] For example, the owner can command by saying "Alexa, play some relaxing music," or "Alexa, tell me the weather today." Echo records these commands and uploads the audio files to Amazon's cloud server.[240] The cloud server translates the audio into text, figures out the best way to respond, transmits that response back to Echo speaker, and the speaker converts the texts back into a spoken response.[241]

But Echo can do so much more than just responding to basic commands.[242] It can control the lights and room temperature; it can connect to and become a remote control for compatible TVs; it can set up alarm clocks and calendar reminders; it can make purchase orders on Amazon; it can generate a to-do list; it can retrieve cooking recipes for boeuf bourguignon and chocolate chip cookies; it can flip a coin and roll a die; it can order coffee, pizza, or a Lyft ride; and it can even have a conversation with a interested user.[243] The brilliant minds at Amazon are enlarging Echo's capabilities day-by-day. Just recently, Echo revolutionized and redefined the concept of "home

235. *See* Sarah Perez, *39 Million Americans Now Own a Small Speaker, Report Claims*, TECHCRUNCH (Jan. 12, 2018), https://techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims/ [https://perma.cc/GQ9G-D43C].

236. *See id.*

237. *See* Andrew Gebhart Crist, *Everything You Need to Know About the Amazon Echo*, CNET (Sept. 21, 2018), https://www.cnet.com/how-to/amazon-echo-alexa-everything-you-need-to-know/ [https://perma.cc/9J89-Z7WF].

238. *Id.*

239. *See id.*

240. *See id.*

241. *See id.*

242. *See* Taylor Martin & David Priest, *The Complete List of Alexa Commands So Far*, CNET (Sept. 24, 2018), https://www.cnet.com/how-to/amazon-echo-the-complete-list-of-alexa-commands/ [https://perma.cc/2DGA-3V2F].

243. *See id.*

phone" by enabling users to call friends and families with just a verbal command.[244] The user now can simply say "Alexa, call my friend Smith," and Alexa will dial the phone number saved as "my friend Smith" in the user's phone book. Needless to say, Echo diligently records and uploads a tremendous amount of intimate information about its users' lives. Where does all that information go? Amazon servers.[245]

Obviously, the government cannot search an Echo device itself without a warrant, as obtaining the device requires physically entering into someone's home and thus requires a warrant. But can the government go to Amazon's headquarters and demand Amazon to turn over the database on its cloud servers? Under a straightforward application of the third-party doctrine, yes—Amazon is a third party to which the users voluntarily and knowingly send information. But based on *Riley* and *Carpenter*? Probably not.

Whereas the phone numbers collected in *Smith* are merely individual strings of numbers that bear no other significance, the information Echo records and transmits to Amazon servers is something else. The calling feature allows Amazon to access user's contact list; the ordering/reordering feature allows Amazon to know the user's payment information and shipping addresses; search functions reflect the user's personal preference; and on top of everything, Echo transmits clips about its user's private life *at home*.[246] Thus, Echo is more akin to the phone in *Riley*. With its capability to transmit not only an exhaustive volume of information, but also sensitive and personal details of a user's private life, the recordings that Echo turns over to Amazon cloud servers is both qualitatively and quantitatively different from the phone numbers in *Smith*. This type of information is exactly what the Court would call "the privacies of life," and it is the very type of information the Fourth Amendment seeks to protect. Thus, any attempt to obtain such information from Amazon's servers would constitute a search within the meaning of the Fourth Amendment.

Echo is a world of difference from a pen register—from a single-function recording device to a sophisticated smart home system with new functions constantly implemented. This difference is exactly what the *Carpenter* majority would call a "seismic shift" in technology.[247] Therefore, the type of

244. *See* Maggie Tillman, *What Is Amazon Alexa Calling and Messaging and How Does It Work?*, POCKET-LINT (Sept. 19, 2018), https://www.pocket-lint.com/smart-home/news/amazon/140981-amazon-alexa-calling-and-messaging-what-is-it-how-does-it-work-and-where-can-you-use-it [https://perma.cc/DRQ9-LXQW].

245. *See* Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ [https://perma.cc/HU28-2HK8].

246. *See* Crist, *supra* note 237.

247. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

information Echo records is closer to the *Carpenter* extreme of the spectrum and is not covered by the third-party doctrine.[248]

When this Note was under production, Echo recordings were involved in a double-murder case in New Hampshire.[249] Law enforcement believed that an Echo located in the two victims' kitchen might have "picked up 'audio recordings capturing the attack' and 'any events that preceded or succeeded the attack.' "[250] In line with the analysis above, the government in this case had to show *probable cause* before the court issued an order of search allowing the government to demand information from Amazon servers.[251] This case perfectly exemplified that obtaining Echo recordings constitutes a search and is not covered by the third-party doctrine.

3. Credit Card Records

The third technology discussed advances *Miller*'s checkbook by leaps and bounds—credit cards. *Miller* was decided back when people were carrying around cash and checkbooks. Needless to say, the world has changed since the invention of credit cards. Each time a card holder makes a transaction, the nature of that transaction will be recorded, including the vendor's name, the amount of the transaction, the time of the transaction to the exact second, and the location where the transaction took place. There is, arguably, "a world of difference" between the check records in *Miller* and credit card records.[252]

First, the two records differ in their pervasiveness. One has to recognize how frequently credit cards are used nowadays as compared to checks used in the 1970s. Back in the 1970s, people used checks for paying salaries and rent but not on miscellaneous transactions, such as buying a cup of coffee or a blueberry muffin.[253] Check transactions only constituted a little portion of an individual's overall transaction records. In the present day, however, credit cards are used on a full range of things.[254] Whether an individual buys a can of soda, a candy bar, or an expensive car, they can pay for all of them with a credit card.

248. *Id.*

249. *See* Zack Whittaker, *Judge Orders Amazon to Turn over Echo Recordings in Double Murder Case*, TECHCRUNCH (Nov. 14, 2018), https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/ [https://perma.cc/9UAL-NRLV].

250. *Id.*

251. *See id.*

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

253. Interview with James Dempsey, Dir., Berkeley Ctr. for Law & Tech., in Berkeley, Cal. (Nov. 2018) (transcript on file with author).

254. *See* Jason Steele, *Payment Method Statistics*, CREDITCARDS (May. 30, 2018), https://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php [https://perma.cc/6R96-QBEJ].

Second, credit card records and check records are very different in nature. The check records in *Miller*, as the *Carpenter* Court recognized, did not have a "revealing nature."[255] A credit card record, on the other hand, can potentially reflect a card holder's daily routine: getting a cup of coffee and bagel for breakfast, taking an Uber to the workplace, shopping on Amazon.com for cat litter, buying a salad for lunch, getting another coffee in the afternoon, more shopping online, buying groceries from Wholefoods, and having a drink at a bar before heading back home, and so on. The vast amount of information a credit card record can reveal is frightening, as it permeates through every aspect of the card holder's daily life.

Third, checks cannot track location, while credit cards can. In fact, credit card companies and banks constantly monitor the location where transactions take place to detect potential fraudulent transactions.[256] Credit card companies monitor by looking for unusual activities and unusual transactions.[257] However, to know what is *unusual*, they must first know what is usual, e.g., in which cities the card is being used, which store the card holder frequents, and the typical range of the amount spent on the card.[258] For example, if a card holder lives in the Bay Area and has been using the card predominantly in that location, a sudden transaction in Loxahatchee, Florida, is likely fraudulent. By the same token, if a card holder typically spends no more than $2,000, a $12,500 transaction will likely trigger some alert. How do the credit card companies do that? Depending on the technologies used, companies either do a fully automated fraud-alert process or a machine-human combined process to combat fraud.[259] The process involves analyzing massive amounts of credit card transaction data to learn patterns for each individual card holder to be

255. *Carpenter*, 138 S. Ct. at 2219. Chief Justice Roberts found that cell-site location information distinguishes from the records in *Smith* and *Miller* due to its "revealing nature." In particular, he characterized cell-site location information as "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 2220.

256. For example, Bank of America has a global information security team that monitors all the activities 24/7 to detect fraudulent transactions. *See Here's What You Need to Know (and Do) to Stay as Safe as Possible*, BANK OF AM., https://www.bankofamerica.com/privacy/overview.go [https://perma.cc/GZ26-F7PA] (last visited Dec. 17, 2018). Credit card companies and banks are dedicated to catching fraudulent behaviors, as the card owners are only responsible for up to $50 for any fraudulent transactions—the rest is on the credit card companies and the banks. *See* Selena Maranjian, *How do Credit Card Companies Spot Fraud?*, MOTLEY FOOL (Sept. 29, 2017), https://www.fool.com/credit-cards/2017/09/29/how-do-credit-card-companies-spot-fraud.aspx [https://perma.cc/HF6D-9SJ4].

257. *See* Maranjian, *supra* note 256.

258. *See id.*

259. *See id.*

able to recognize and pick out transactions that "might be fraud."[260] When potential fraud is detected, the credit card companies either call, or text, the card holders to alert them. At the same time, the companies decline the suspicious transaction and suspend the card until the card holders approve or disapprove the suspicious transaction.[261] This means that credit card companies and banks are monitoring and tracking card holders' every move and every transaction.[262]

In a way, credit card records are more or less akin to cell-site location information in that they chronically track the movement of card holders and record location information whenever a transaction has been made. If card holders elect not to use this form of payment, they are potentially subject to various forms of "penalties," such as being robbed for carrying too much cash, losing money to fraudulent transactions, etc. They are also likely be marginalized by modern society—a society that runs and relies on this type of technological advancement.[263] Again, given the importance of using credit cards, and the revealing nature of credit card reports, credit card report information should also be considered as being one of the "privacies of life," entitling it to the plethora of protections afforded by the Fourth Amendment. Thus, obtaining credit card records should constitute a search.

Adding up all three differences together, it is fair to say that credit card records are qualitatively and quantitatively different from the check records in *Miller*. Credit card records not only have a much higher volume of personal information, they are also a chronicle of each card holder's transactions and location data. These meaningful differences are the "world of difference" brought by the seismic shifts in credit card technology.[264] Thus, according to *Carpenter*'s holding, credit card records are not covered by the third-party doctrine.

---

260. Steve Adcock, *How Credit Card Fraud Detection Works*, THINKSAVERETIRE (Sept. 14, 2015), https://thinksaveretire.com/how-credit-card-fraud-detection-works/ [https://perma.cc/FKE9-4NJX]; *see also* Kimberly Palmer, *How Credit Card Companies Spot Fraud Before You Do*, U.S. NEWS (July 10, 2013), https://creditcards.usnews.com/articles/how-credit-card-companies-spot-fraud-before-you-do [https://perma.cc/962M-QDT3].

261. *See* Palmer, *supra* note 260.

262. *See id.*

263. *See* Christy Rakoczy Bieber, *Why Is Credit Important?*, CREDIT KARMA (Dec. 4, 2018), https://www.creditkarma.com/advice/i/why-is-credit-important/ [https://perma.cc/7WDL-ZJE6] (listing various reasons why having a good credit score is important in life); Liz Weston, *Why Your Credit Score Is Important*, NERDWALLET (Oct. 1, 2018), https://www.nerdwallet.com/blog/finance/great-credit-powerful-tool/ [https://perma.cc/UJ9P-SZ88] (characterizing credit score as "an integral part of our financial lives").

264. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

V. CONCLUSION

Carpenter is no doubt another landmark case in the history of data privacy cases. The decision shows that the Court is moving further away from a "mechanical interpretation" of the Fourth Amendment to be more adaptive to the digital era.[265] Looking back to the path that the Court has paved, from the infrared technology in *Kyllo*, to the GPS in *Jones*, to the cell phone in *Riley*, the Court has been careful not to allow government's newest and most sophisticated, "progress[es] of science" to erode individuals' privacies.[266] It is therefore no surprise that *Carpenter* followed that exact path.

Carpenter is also a landmark decision for redefining the limit of the third-party doctrine. Confronted with the seismic shift in technology, the Court significantly limited the applicability of what has been considered a categorical rule. The *Carpenter* decision grounded the third-party doctrine to the limited, less-revealing types of personal information in *Miller* and *Smith*. Any information sought after that is qualitatively and quantitatively different and is not covered by the third-party doctrine.

The looming question in the post-*Carpenter* era is no doubt "where we draw the line"? If location information is considered sensitive because of the inferences that can be drawn, what about other information that is arguably sensitive, like internet search terms? Home surveillance technologies? Pet cameras? Where does the slippery slope end remains to be an important piece of puzzle in the Fourth Amendment jurisprudence. At least for now, the Court's consistency in expanding the scope of Fourth Amendment protections to account for powerful technologies elucidates the direction that the Court is going forward: The privacies of life are not at the mercy of technology advancements in the digital era.

265. *Id.* at 2214.
266. *Id.* at 2223.