SEARCHES AND SEIZURES – FOURTH AMENDMENT AND REASONABLENESS IN GENERAL: PROTECTION OF PRIVACY INTERESTS IN THE DIGITAL AGE

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

ABSTRACT

The law must evolve to remain applicable in the face of vast new technological landscapes. Created during colonial times, the Fourth Amendment's initial concern was protecting American citizens from officers physically invading their homes, supported merely by general warrants that needed no probable cause. The Fourth Amendment's protections have been judicially expanded to protect privacy interests which society recognizes as reasonable. In the cyber age, a debate rages about what precisely society recognizes as a reasonable expectation of privacy regarding digital data.

Nearly every American adult owns a cell phone—the device at the heart of *Carpenter v. United States*. Law enforcement used cell site location information ("CSLI") generated by petitioner Carpenter's cell phone to place him at the scene of, ironically enough, a string of robberies at Radio Shacks and T-Mobile stores. Law enforcement followed the procedure laid out in the Stored Communications Act and obtained a court order for the CSLI records. Petitioner Carpenter objected to his CSLI records being obtained without a search warrant, asserting it was a violation of his Fourth Amendment rights. The Supreme Court *held* that petitioner Carpenter had a protected Fourth Amendment privacy interest in the CSLI, marking a sharp divergence from existing case law that asserted a person cannot have a cognizable privacy interest in data shared with a third party. Justices Kennedy, Thomas, Alito, and Gorsuch strongly dissented, arguing the holding disregarded existing precedent, placed undue restrictions on law enforcement, and created illogical dichotomies in the law. The dissenting justices harshly criticized the *Katz* reasonableness test, on which the majority relied in its opinion.

Carpenter is narrow in its scope but creates broad opportunities for practitioners in North Dakota, and nationwide, to argue for the suppression of digital data, which the Fourth Amendment previously could not have protected due to the third-party doctrine. This precedent is critical to protecting privacy in an age where it is necessary to use technology to participate in modern society, and nearly all devices mere use involves sharing data with third parties.

I. FACTS 198
II. LEGAL BACKGROUND 200
A. JUDICIAL INTERPRETATION OF THE FOURTH AMENDMENT 200
B. THE *KATZ* REASONABLENESS TEST FOR PROTECTED PRIVACY INTERESTS 201
C. FOURTH AMENDMENT PROTECTIONS IN MODERN SOCIETY 202
D. THE THIRD-PARTY DOCTRINE 205
E. REQUISITE CONNECTION FOR LEGITIMATE PROPERTY INTERESTS 207
F. THE STORED COMMUNICATIONS ACT 208
III. ANALYSIS 208
A. THE MAJORITY OPINION 209
B. DISSENTING OPINIONS 211
1. *Justice Kennedy's Dissent* 211
2. *Justice Thomas's Dissent* 212
3. *Justice Alito's Dissent* 213
4. *Justice Gorsuch's Dissent* 214
IV. IMPACT 216
V. CONCLUSION 219

I. FACTS

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and T-Mobile stores in Detroit.[1] One of the men confessed that the group had robbed nine different stores over the past four months and gave the FBI the cell phone numbers of some of the accomplices.[2] The FBI reviewed call records to identify additional numbers that the accomplices called during the timespan of the robberies.[3]

1. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
2. *Id.*
3. *Id.*

Based on information provided by the FBI, prosecutors were given court orders to obtain suspects' cell records under the Stored Communications Act.[4] Federal magistrate judges issued two orders directing petitioner Timothy Carpenter's wireless carriers to disclose cell site location information ("CSLI") at both call origination and termination during the four-month period.[5] In sum, the government received 12,898 location points cataloging Carpenter's movements from the wireless carriers – the location information showed that Carpenter's phone was near four of the robbery locations when the robberies were committed.[6]

Carpenter was charged with six counts of robbery and six counts of carrying a firearm during a crime of violence.[7] At trial, seven of Carpenter's accomplices named him as the organizer of the robberies.[8] Additionally, an FBI agent served as an expert witness at trial, explaining that every time a cell phone connects to a wireless network, the carrier logs a time-stamped record of the cell site and particular sector used.[9] Law enforcement then used these records to create a map placing Carpenter's phone near four of the charged robberies.[10] The government felt this piece of evidence "clinched the case" by confirming Carpenter's presence near the robberies.[11]

Carpenter moved to suppress the CSLI, arguing the seizure violated the Fourth Amendment because the government did not obtain a warrant supported by probable cause before obtaining the records.[12] The district court denied the motion.[13] Carpenter was convicted on all counts but one firearm charge and sentenced to over 100 years in prison.[14] Carpenter appealed, and the Sixth Circuit affirmed.[15] The Sixth Circuit reasoned that Carpenter lacked a reasonable expectation of privacy in the location where his information was

4. *Id.* (permitting the government to compel disclosure of certain telecommunications records when they "are relevant and material to an ongoing criminal investigation").
5. *Id*.
6. *Id.* at 2212–2213.
7. *Carpenter*, 138 S. Ct. at 2212.
8. *Id.*
9. *Id.* at 2212–13.
10. *Id.*
11. *Id*. at 2213.
12. *Id.* at 2212.
13. *Carpenter*, 138 S. Ct. at 2213.
14. *Id.*
15. *Id.*

collected because he had voluntarily shared that information with his cell phone carriers.[16] The Supreme Court granted certiorari and reversed.[17]

II. LEGAL BACKGROUND

The Supreme Court has continued to interpret and expand the scope of Fourth Amendment protections. Initially, the Fourth Amendment was inextricably bound with property concepts: it protected against unreasonable searches, seizures, and intrusions of a person's physical being, home, and material possessions.[18] But as advancing technology has allowed for more remote government searches and invasions into formerly private spheres, the Supreme Court has grappled with the application of the Fourth Amendment in a world replete with technology that the founders could not have anticipated.[19] Recognizing this reality, the Supreme Court expanded the Fourth Amendment in the landmark case *Katz v. United States*[20] in 1967, declaring that the Fourth Amendment also protected individual privacy interests.[21]

A. JUDICIAL INTERPRETATION OF THE FOURTH AMENDMENT

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 . . . ."[22] The Fourth Amendment has been judicially interpreted as protecting the privacy and security of individuals against arbitrary invasions by government officials.[23] Specifically, the Founding generation created the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[24]

The Fourth Amendment asserts the right to be free of unreasonable searches and seizures but makes no mention of how this right is supposed to be enforced.[25] To supplement the bare text of the Fourth Amendment, the

16. *Id.*
17. *Id.*
18. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928).
19. *See, e.g.*, *id.* at 466.
20. 389 U.S. 347 (1967).
21. *Katz*, 389 U.S. at 351.
22. U.S. CONST. amend. IV.
23. *See* Camara v. Mun. Court, 387 U.S. 523, 528 (1967).
24. *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014).
25. U.S. CONST. amend. IV.

Supreme Court created the exclusionary rule, which Justice Alito recently defined as "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation."[26]

The first time the Supreme Court encountered a Fourth Amendment challenge to a search involving then novel technology occurred in 1927, when an electric spotlight was used to illuminate a boat "running rum" during prohibition.[27] However, the Court barely considered the implications of the new technology that facilitated the search – and devoted almost no analysis to the spotlight's impact.[28]

The following year, in *Olmstead v. United States*,[29] the Supreme Court considered a Fourth Amendment challenge to evidence gathered via a wiretap.[30] The Court explained that its construction of Fourth Amendment protections at the time was firmly rooted in property rights, reasoning that a Fourth Amendment violation could not exist without an actual search or seizure of a person, their material effects, or a physical invasion of a person's home.[31] Accordingly, because the wiretap was conducted without a physical trespass, the Fourth Amendment's protections were not invoked and the Supreme Court affirmed the convictions.[32]

The Supreme Court's interpretation of Fourth Amendment protections, and the application of the exclusionary rule in criminal proceedings, remained intertwined with concepts of property law until *Olmstead* was overturned by *Katz* in 1967. From *Katz* onward, the Supreme Court has continued to recognize that the Fourth Amendment's protections encompass more than solely property rights and in fact protect individual privacy.[33]

B. THE *KATZ* REASONABLENESS TEST FOR PROTECTED PRIVACY INTERESTS

Katz expanded the conception of the Fourth Amendment beyond guarding only against physical intrusions.[34] In *Katz*, FBI agents attached a listening device to the outside surface of a public telephone booth, which was used to

26. Davis v. United States, 564 U.S. 229, 231–32 (2011).
27. *See* United States v. Lee, 274 U.S. 559, 563 (1927).
28. *See id*.
29. 277 U.S. 438 (1928).
30. *Olmstead*, 277 U.S. at 455.
31. *Id*. at 466.
32. *Id*.
33. *See* United States v. Jones, 565 U.S. 400 (2012).
34. Katz v. United States, 389 U.S. 347, 351 (1967).

record defendant Katz transmitting illegal wagering information.[35] Katz was convicted on the strength of the evidence obtained from the recording device.[36] When Katz challenged the recording as a Fourth Amendment violation, both the district court and the court of appeals disagreed, reasoning that because the agents had not physically entered the phone booth, there could be no constitutional violation.[37]

The Supreme Court disagreed, reasoning that a person alone in a telephone booth had a reasonable expectation that his communications would not be broadcast to the world.[38] In so reasoning, the Supreme Court established the reasonable expectation of privacy test, which has yet to be supplanted by a new privacy doctrine.[39] Ultimately, the Supreme Court shifted away from focusing on property rights and established that the Fourth Amendment "protects people, not places."[40] The *Katz* test is articulated in Justice Harlan's concurrence as having "a twofold requirement."[41] Specifically, the rule is that a person must first have exhibited a subjective expectation of privacy.[42] Second, the person's subjective expectation of privacy must be one that society is prepared to recognize as "reasonable."[43]

C. FOURTH AMENDMENT PROTECTIONS IN MODERN SOCIETY

The Supreme Court has continued to grapple with the application of the Fourth Amendment in a world increasingly driven by technology. In *United States v. Jones*, for example, the Supreme Court further refined the scope of Fourth Amendment protections in our technologically advanced society.[44] In *Jones*, agents installed a GPS tracking device on the vehicle of the defendant because he was under suspicion of drug trafficking.[45]

The district court denied the defendant's motion to suppress the GPS location evidence in part.[46] The district court suppressed data obtained from the tracker while it was parked inside the defendant's garage, reasoning that

35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.*
40. *Katz*, 389 U.S. at 351.
41. *Id.* at 361 (Harlan, J., concurring).
42. *Id.*
43. *Id.*
44. United States v. Jones, 565 U.S. 400, 403 (2012).
45. *Id.* at 404.
46. *Id.*

he had a justifiable privacy interest at his residence.[47] However, the district court deemed data obtained when the defendant's vehicle was on public roads admissible, asserting he had no reasonable expectation of privacy in his movements when in public.[48]

The court of appeals disagreed. The court of appeals applied the *Katz* test and reasoned that the government's actions infringed upon the defendant's reasonable expectation of privacy in his movements.[49] Accordingly, the court of appeals reversed the defendant's conviction, holding that the district court erred in admitting even part of the GPS location data.[50] The Supreme Court granted certiorari, and affirmed the court of the appeals.[51]

Justice Scalia delivered the majority opinion of the Court. Throughout the opinion, Justice Scalia focused on physical trespass caused when law enforcement placed the tracker on the vehicle, stating, "the Government physically occupied private property for the purpose of obtaining information."[52] This, the opinion asserted, constituted a classic search under the Fourth Amendment, which is closely tied to property rights.[53] This raises serious questions about whether the Supreme Court has completely divorced itself from property rights impacting Fourth Amendment analyses in favor of broader concepts of reasonableness and privacy rights.

The majority opinion in *Jones* asserted that the *Katz* reasonableness test may not be the exclusive test for determining Fourth Amendment violations.[54] Instead, the majority asserted that when a classic trespass is present, there is no need to resort to the *Katz* test. In fact, the opinion found that applying the *Katz* test "leads us needlessly into additional thorny problems."[55] The majority predicted the question presented to the Court in *Carpenter*, stating, "It may be that achieving the same result [of traditional surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[56]

---

47. *Id.*
48. *Id.* at 404–05.
49. *Id.* at 406.
50. *Jones*, 565 U.S. at 404.
51. *Id.* at 431.
52. *Id.* at 404–05.
53. *Id.*
54. *Id.* at 411–12.
55. *Id.*
56. *Jones*, 565 U.S. at 412.

The majority opinion strongly differed from Justice Alito's concurrence, which was joined by Justices Ginsburg, Breyer, and Kagan. This concurrence focused on the duration of the search rather than the presence of a physical trespass.[57] The concurrence criticized the majority's originalist approach as outdated in the face of modern technologies.[58] Specifically, the concurrence asserted that the majority's grounding of its opinion in "18th-Century tort law" was ironic for a case turning on the use of GPS, a 21st-century surveillance technology.[59] Furthermore, the concurrence characterized the majority's reasoning as unwise and highly artificial.[60]

The concurrence asserted that the majority's reasoning "largely disregards what is really important . . . and instead attached great significance to something that most would view as relatively minor."[61] The concurrence viewed the use of GPS for the purpose of long-term tracking as the real concern, and characterized the trespass affected by attaching the GPS to the undercarriage of Jones' vehicle as comparatively minor.[62] The concurrence asserted this misguided approach would lead to incongruous results, where police attaching a GPS tracker to a vehicle for even a brief period could result in a Fourth Amendment violation, but long-term monitoring accomplished without committing a physical trespass would not.[63] Instead, Alito's concurrence asserted the *Katz* reasonableness test is preferable because it avoids such incongruous results.[64] However, Justice Alito did acknowledge that judges are apt to "confuse their own expectations of privacy with those of the hypothetical reasonable person to which the Katz test looks."[65]

The true focus of the concurrence was the duration of the search.[66] While the opinion did not draw a hard line as to when the tracking of the vehicle became a search, it argued "surely the line was crossed before the 4-week mark."[67] Therefore, it is unclear if the concurrence would have found a protected privacy interest in one's movements in public, and instead seemed to assert that warrantless continuous tracking of a suspect's movements by law

57. *Id.* at 418–31 (Alito, J., concurring).
58. *Id.* at 418.
59. *Id.*
60. *Id.* at 419.
61. *Id.* at 425.
62. *Jones*, 565 U.S. at 425.
63. *Id.*
64. *Id.* at 427.
65. *Id.*
66. *Id.* at 431.
67. *Id.* at 430.

enforcement is unreasonable.[68] The concurrence reasoned that use of technology like GPS had allowed law enforcement to track every movement of an individual's vehicle over a long period in a way that simply would not be possible using traditional surveillance techniques.[69] This kind of extended tracking of an individual's movements via technological means was precisely the issue in *Carpenter*.[70]

Another seminal case illustrating the Supreme Court's evolving Fourth Amendment jurisprudence in a society increasingly driven by new technologies is *Riley v. California*. Like *Carpenter*, that case turned on digital data evidence gathered from cell phones. In two joined cases, both defendants had their cell phones seized incident to arrests, the contents of which law enforcement searched without a warrant.[71] The Supreme Court weighed the degree to which such a search intrudes on an individual's privacy against legitimate government interests in effective law enforcement.[72]

The Court asserted that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person" because they can store millions of pages of text, thousands of pictures, or hundreds of videos, which raise several "interrelated privacy consequences."[73] In sum, cell phones are pervasive in society, reveal more in combination than any single record, and convey far more information than previously possible.[74] Echoes of these concerns can be heard in the majority opinion in *Carpenter*, which states that cell phones are indispensable to modern society and their records often hold the "privacies of life."[75] Accordingly, the Court held in *Riley v. California* that law enforcement must obtain a search warrant before searching the digital contents of a cell phone.[76] As such, this precedent was a direct precursor to *Carpenter*.

D. THE THIRD-PARTY DOCTRINE

Despite the holding in *Katz*, the Fourth Amendment's protections in modern society have not always been expanded in response to technological

68. *See Jones*, 565 U.S. at 430.
69. *See id.*
70. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
71. Riley v. California, 134 S. Ct. 2473, 2477 (2014).
72. *Id.* at 2478.
73. *Id.*
74. *Id.* at 2479.
75. *Carpenter*, 138 S. Ct. at 2211–18.
76. *Riley*, 134 S. Ct. at 2495.

advances. One notable limitation on Fourth Amendment protection is the third-party doctrine. The Supreme Court established the third-party doctrine in *United States v. Miller*[77] and *Smith v. Maryland*.[78] This exception asserts that a person cannot have a protected privacy interest in information voluntarily turned over to a third party.[79]

The roots of the third-party doctrine are found in *Miller*. The government undertook an investigation of Miller for tax evasion and subpoenaed several banks seeking records of his canceled checks, deposit slips, and monthly statements over the course of many months.[80] Miller unsuccessfully challenged the subpoena as a Fourth Amendment violation in the district court.[81] On appeal, the Supreme Court asserted that Miller could not assert ownership or possession over the records because they were "all business records of the banks."[82] The Court further reasoned that the very nature of the records confirmed Miller's "limited expectation of privacy" because they were not confidential communications.[83] Accordingly, the Court held that the defendant had no reasonable expectation of privacy in financial records held by a third-party bank because he had undertaken the risk that the information would be conveyed to the government.[84]

In *Smith*, the government had a telephone company install a device that recorded outgoing phone numbers dialed on a landline telephone.[85] Without a warrant, the government used this device to identify the numbers that a suspect in a robbery was dialing.[86] On the strength of the evidence gathered by the device, the suspect was indicted and convicted of robbery.[87] Smith moved to suppress the evidence gathered by the device on Fourth Amendment grounds, but his motion was denied by the district court.[88]

The Maryland Court of Appeals affirmed the conviction, reasoning that Smith did not have a constitutionally protected reasonable expectation of pri-

77. 425 U.S. 435 (1976).
78. 442 U.S. 735 (1979).
79. *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 440–43.
80. *Miller*, 425 U.S. at 440.
81. *Id.*
82. *Id.*
83. *Id*.
84. *Id.* at 443.
85. Smith v. Maryland, 442 U.S. 735, 737 (1979).
86. *Id.*
87. *Id.* at 736.
88. *Id.*

vacy in the numbers dialed on a telephone, and therefore no search had occurred.[89] The Supreme Court affirmed, reasoning that the defendant had no expectation of privacy because the information was conveyed to the third-party telephone company, and further asserted that such an expectation of privacy was not reasonable under the *Katz* test.[90]

The tension between the third-party doctrine and the *Katz* reasonableness test is not apparent in *Smith* and *Miller*. The Court decided that because the parties had voluntarily shared the disputed information with third parties, their expectation of privacy in that information was unreasonable. However, in *Carpenter v. United States*, the Court made clear that the two doctrines are hardly inextricable.[91] The *Katz* test protects privacy interests an individual has sought to preserve as private and that society is prepared to recognize as reasonable. *Carpenter* has made clear that sharing information with third parties does not always render that privacy expectation unreasonable.[92]

E. REQUISITE CONNECTION FOR LEGITIMATE PROPERTY INTERESTS

In *Minnesota v. Carter*,[93] the Supreme Court interpreted the standards set forth in *Miller* and *Smith* as placing necessary limits on Fourth Amendment property interests when the person asserting them lacks the requisite connection to the property.[94] The requisite connection principle is straightforward: it asserts that for a person's objection to the search of a place to be effective, she or he must have a requisite connection to the place.[95] Put simply, individuals have a greater expectation of privacy in things that belong to them.

In *Carter*, a police officer observed respondents bagging cocaine at a third party's apartment through a window.[96] Respondents argued the officer's observation was an unreasonable search under the Fourth Amendment.[97] The Court reasoned that because respondents were merely present with the consent of the homeowner, rather than overnight guests or the apartment's renters, they did not have a legitimate expectation of privacy.[98] Accordingly,

89. *Id.*
90. *Id.* at 745–46.
91. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
92. *Id.*
93. 525 U.S. 83 (1998).
94. *Carter*, 525 U.S. at 98.
95. *See id.*
96. *Id.*
97. *Id.* at 87.
98. *Id.* at 83.

the Supreme Court held that any search that may have occurred did not violate respondents' Fourth Amendment rights because they lacked the requisite connection to the space to have a legitimate expectation of privacy.[99]

F. THE STORED COMMUNICATIONS ACT

The Stored Communications Act allows the government to compel the disclosure of certain telecommunications records when law enforcement shows reasonable grounds for believing records are relevant and material to an ongoing investigation.[100] This standard is substantially lower than probable cause.[101] Under this act, prosecutors can apply for and receive court orders compelling the disclosure of these telecommunication records, such as CSLI.[102] This compulsory process was followed by law enforcement in *Carpenter* in gathering the CSLI, but because its standard falls well short of probable cause, its application in *Carpenter* was held to violate the Fourth Amendment when used to gather historical cell-site records.

III. ANALYSIS

In *Carpenter v. United States*, the Supreme Court had to balance two fundamental and conflicting principles of Fourth Amendment jurisprudence – the *Katz* reasonableness test and the third-party doctrine.[103] Ultimately, a narrow majority declined to extend the third-party doctrine to include CSLI, asserting that Carpenter's exposure of his location data to his wireless carriers was not truly voluntary.[104] Furthermore, the majority opinion's concern that CSLI could be used to create a continuous chronicle of a suspect's location indicated that the Court did not believe such an intrusion into individual privacy could be justified without a warrant supported by probable cause.[105] In contrast, Justices Kennedy, Thomas, Alito, and Gorsuch all filed dissenting opinions.[106]

---

99. *Id.*
100. 18 U.S.C. § 2703(d) (2012).
101. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
102. *See id.*
103. *See id.* at 2219–20.
104. *Id*. at 2220.
105. *See id*. at 2217.
106. *Id.* at 2224–72.

A. THE MAJORITY OPINION

In *Carpenter,* the Supreme Court had to balance the *Katz* reasonableness test with the third-party doctrine in a case where modern technology gave the government "the ability to chronicle a person's past movements through the record of his cell phone signals."[107] While the third-party doctrine certainly appeared to apply at first glance, the Supreme Court declined to extend the third-party doctrine to digital CSLI data for two reasons. First, cell phones are "'such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society."[108] Second, the Supreme Court found that the third-party doctrine did not apply because cell phones log location information as part of their regular operation without any affirmative act on the user's part.[109]

The Court explained that personal location information gathered from CSLI was not truly knowingly or voluntarily shared, removing it from the scope of the third-party doctrine.[110] The Court reasoned that CSLI detailed a person's every movement at every moment, regardless of whether that person affirmatively disclosed any information to his or her wireless carrier.[111] Therefore, the Court concluded that a cell phone user's exposure to CSLI tracking is not truly voluntary because cell phones are both a necessity of modern life and create CSLI records without an affirmative act on the user's part.[112] The majority opinion further distinguished the third-party doctrine established in *Smith* and *Miller* from the situation presented in *Carpenter* by asserting that the former dealt with "limited types of personal information" that vastly differed from a "chronicle of location information."[113] For these reasons, the Court held that the third-party doctrine was not applicable to CSLI.

The Court reaffirmed that a person "does not surrender all Fourth Amendment protections by venturing into the public sphere," quoting its opinion in *Katz*.[114] The Court's holding built directly on Justice Alito's concurring opinion in *Jones*, which asserted that attaching a GPS locator to a car without a warrant to track personal movements over an extended period

107. *Carpenter*, 138 S. Ct. at 2213, 2216.
108. *Id.* at 2210 (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).
109. *Id.* at 2220.
110. *Id.*
111. *Id.* at 2220.
112. *Id.*
113. *Carpenter*, 138 S. Ct. at 2219–20.
114. *Id.* at 2217.

of time was a Fourth Amendment violation.[115] The Court reasoned that CSLI was reaching near-GPS level precision in its ability to track movements, and further asserted that the "retrospective quality" of the data gave police access to information previously unknowable.[116] Indeed, the Court expressed Orwellian concerns about the ubiquity of cell phones coupled with the fact that CSLI was becoming ever more precise.[117] The majority opinion espoused concerns that CSLI would "give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."[118] Prior to the digital age, law enforcement might have pursued a suspect for a brief period, but doing so for any extended period was rarely undertaken due to the difficulty and cost.[119] The Court asserted for this reason society had a reasonable expectation that law enforcement agents "would not—and indeed, in the main, simply could not—secretly monitor and catalog every single movement."[120]

The Court employed the *Katz* reasonableness test and asserted that allowing government to access cell-site records contravened this reasonable expectation. The majority opinion dismissed the dissents' concerns about the holding impeding law enforcement, asserting the exigent circumstances doctrine would allow law enforcement access to CSLI without a search warrant when the exigencies of the situation make a warrantless search objectively reasonable under the Fourth Amendment.[121]

Accordingly, the Supreme Court held that CSLI surveillance violated the Fourth Amendment absent a warrant supported by probable cause, and reversed and remanded.[122] The majority took pains to express its decision was a narrow one, with no "view on matters not before us."[123] The Court asserted this narrowness was necessary to ensure the Court did not "embarrass the future," impliedly taking into consideration the ever-present rapid advancement of modern technologies.[124]

---

115. *Id.* at 2218.
116. *Id.*
117. *Id.* at 2119.
118. *Id.* at 2210.
119. *Carpenter*, 138 S. Ct. at 2217.
120. *Id.*
121. *Id.* at 2222.
122. *See id.*
123. *Id.* at 2220.
124. *See id.*

B. DISSENTING OPINIONS

Justices Kennedy, Thomas, Alito, and Gorsuch each strongly dissented from the majority. Justice Kennedy's dissent, in particular, voiced concerns that *Carpenter's* holding jeopardized congressionally authorized criminal investigations and placed undue restrictions on the federal government and law enforcement nationwide.[125] All of the dissenting justices expressed concerns about *Carpenter's* holding further divorcing the Fourth Amendment from its foundation in the concept of personal property. Justices Thomas, Alito, and Gorsuch all harshly critiqued the *Katz* reasonableness test. Justice Gorsuch advocated for eliminating both the third-party doctrine and the *Katz* test in favor of a positive law model.

1. *Justice Kennedy's Dissent*

Justice Kennedy's dissent focused on the fact that in *Carpenter*, the government acquired records through a congressionally authorized investigative process.[126] Furthermore, his dissent argued that because customers "do not own, possess, control, or use the records," they could not have a reasonable expectation that those records would not be disclosed pursuant to a lawful compulsory process.[127] Kennedy also mused that the majority's holding vexingly provided greater Fourth Amendment protections to an individual who was the focus of the records being subpoenaed, rather than the party actually being subpoenaed.[128]

Justice Kennedy's dissent also asserted that the *Katz* reasonableness test was in line with the *Carter* requirement of requisite connection for privacy interests. His dissent analogized Katz's use of a phone booth to a hotel room or taxicab, where a person has a reasonable expectation of privacy for the duration of their use of that space.[129] The implication is that Carpenter had too attenuated of a connection to his CSLI records to invoke Fourth Amendment protections, as the records were not stored, maintained, or owned by him.[130] Additionally, Kennedy stated that today's reasonable expectation of

125. *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting).

126. *Id.* at 2224 (asserting that the government may legally obtain a wide variety of business records using compulsory processes authorized by Congress).

127. *Id.*

128. *Id.* at 2256.

129. *Id.* at 2227.

130. *See id.*

privacy is diminished as compared to even thirty years ago.[131] This diminished expectation is due to millions of Americans choosing to share their location on a daily basis, through a variety of location-based services on their phones, sharing their location with friends, and even sharing their location with the greater public on social media platforms.[132]

Kennedy further asserted that *Carpenter's* holding "unhinges Fourth Amendment doctrine from the property-based concepts that have long grouped the analytic framework that pertains in these cases."[133] He argued that CSLI was no different from the kind of business records seen in *Smith* and *Miller*, and thus, customers like Carpenter had no possessory interest in those records because they were turned over to a third party.[134] As such, the dissent characterized the majority's holding as a misapplication of the third-party doctrine.

Justice Kennedy's dissent concluded by characterizing the majority's holding as illogical and frustrating. He expressed fear that the broad principles the majority seemed to be espousing—despite professed narrowness in their application to the case—would lead to the requirement that all subpoenas and other orders compelling the production of documents would require a showing of probable cause.[135] Furthermore, the dissent rearticulated that the majority's opinion created illogical dichotomies in the law, highlighting how existing law allowed law enforcement to acquire records of every credit card purchase and phone call a person made over years.[136] His dissent asserted *Carpenter's* holding was inconsistent with that existing broad authority.[137]

2. *Justice Thomas's Dissent*

Justice Thomas's dissent focused on whose property was searched, rather than whether a search occurred.[138] Thomas reasoned that Carpenter did not merely have too attenuated of an interest in the CSLI records to pass muster under the requisite connection standard, but rather that Carpenter had no interest in the records because they were the property of Sprint and

131. *Carpenter*, 138 S. Ct. at 2232 (Kennedy, J., dissenting).
132. *Id.*
133. *Id.* at 2224.
134. *Id.* at 2233.
135. *Id.* at 2234.
136. *See id*. at 2224.
137. *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting).
138. *Id.* at 2235 (Thomas, J., dissenting).

MetroPCS.[139] Simply put, the government did not search Carpenter's property at all.[140] The records were not his because he did not create them, he could not control them, and he could not destroy them.[141]

Thomas proceeded to criticize the *Katz* test as straying too far from the founders' intent when they drafted the Fourth Amendment, asserting that a search did not mean a violation of someone's reasonable expectation of privacy at the time.[142] He critiqued the *Katz* test for reading the crucial limiting words "persons, houses, papers, and effects" out of the Fourth Amendment, creating an amorphously defined and overbroad concept.[143]

Thomas further characterized the *Katz* test as dangerously circular because the Court is supposed to base its decisions on society's expectations of privacy, and society's expectations of privacy are shaped by the Court's decisions.[144] Thomas characterized the *Katz* test as a failed experiment that had strayed so far from the text of the Fourth Amendment that it ought to be rejected.[145] Thomas concluded his dissent by stating the Court was dutybound to reconsider the *Katz* test.[146]

3. *Justice Alito's Dissent*

Justice Alito began his dissent by noting that while he shared the majority's concern about the effect of new technology on personal privacy, he feared *Carpenter's* holding would do more harm than good.[147] The dissent highlighted the "basic distinction" between an actual search on private premises and an order merely requiring a party to look through its records and produce certain documents.[148] The former was characterized as far more intrusive than the latter.[149] Accordingly, Justice Alito argued probable cause ought to be required for the former, but should not be required by the latter.[150]

Alito espoused concerns that *Carpenter's* precedent opened questions of whether every grand jury subpoena for evidence would have to be supported

139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.* at 2238.
143. *See Carpenter*, 138 S. Ct. at 2238–45 (Thomas, J., dissenting).
144. *Id.* at 2245.
145. *Id.* at 2244–46.
146. *Id.*
147. *Id.* at 2247 (Alito, J., dissenting).
148. *Id.*
149. *Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting).
150. *Id.*

by probable cause, which would stymy investigations.[151] Alito expressed concerns that *Carpenter's* precedent would allow a defendant to object to the search of a third party's property, which Alito characterized as "revolutionary."[152] The dissent further stated that the sharp boundary between personal and third-party rights was blurred by the *Katz* test.[153] Alito interpreted *Miller* and *Smith* not as creating a new doctrine—the third-party doctrine—but instead merely rejecting arguments that, had they been accepted, would have disregarded the text of the Fourth Amendment.[154]

Alito concluded his dissent by pointing out that the Fourth Amendment restricts the conduct of the federal government and the states, but does not apply to private actors.[155] The dissent voiced concerns that the holding in *Carpenter* could encourage the public to think the Court can protect them from the "looming threat to their privacy," which would mislead everyone.[156] Furthermore, Alito stated that holding a part of the Stored Communications Act to be unconstitutional could dissuade Congress from further legislation in the field, leaving the public less protected.[157] Alito concluded his dissent by asserting that the majority's desire to make a statement about privacy in the digital age did not justify the consequences of *Carpenter's* holding.[158]

4. *Justice Gorsuch's Dissent*

In our digital landscape, Justice Gorsuch's dissent pondered the question: "What is left of the Fourth Amendment?"[159] On the subject of the third-party doctrine, Gorsuch quipped:

> Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.[160]

---

151. *Id.*
152. *Id.*
153. *Id.* at 2259.
154. *Id.* at 2260.
155. *Carpenter*, 138 S. Ct. at 2260 (Alito, J., dissenting).
156. *Id.* at 2261.
157. *Id.*
158. *Id.*
159. *Id.* at 2262 (Gorsuch, J., dissenting).
160. *Id.*

Gorsuch outlined three potential responses to the uncertain application of the Fourth Amendment in the digital age.[161] The first asserted option is to ignore the problem, maintain *Smith* and *Miller*, and live with the consequences.[162] However, Gorsuch characterized this as a highly undesirable path. In a society where nearly all private information is shared in some respect with third parties via technology, Gorsuch asserted, "if the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be 'never' seems a pretty unattractive societal prescription."[163]

Second, Gorsuch suggested the Court could drop the third-party doctrine altogether in favor of the *Katz* reasonableness test.[164] However, Gorsuch expressed concerns that this would merely return the Court to "its source" because it was "*Katz* that produced *Smith* and *Miller* in the first place."[165] Gorsuch characterized the current confusion regarding the extent of Fourth Amendment protections as the inevitable destination of the precedent set by the vague *Katz* test.[166]

Third, Gorsuch presented his preferred solution: a Fourth Amendment model based on positive legal rights.[167] The dissent asserted that a traditional approach to a Fourth Amendment analysis asked if "a house, paper, or effect was *yours* under law." Under this more traditional model, Fourth Amendment protections for a person's papers and effects did not disappear because they were shared with third parties.[168] When one person entrusts his or her possessions to another, it constitutes a bailment.[169] The bailee, who holds the property for a certain purpose, normally owes a legal duty to keep the property safe.[170] Gorsuch offered the examples of tossing your keys to a valet or having a neighbor watch your dog when you are on vacation as analogues to third parties having access to our digital data.[171] No one would expect the valet to lend the car to his buddy, or their neighbor to put "Fido up for adoption," asserted Gorsuch.[172] Gorsuch proposed that:

---

161. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
162. *Id.* at 2262.
163. *Id.* at 2263.
164. *Id.* at 2264.
165. *Id.*
166. *Id.* at 2267.
167. *Carpenter*, 138 S. Ct. at 2267–68 (Gorsuch, J., dissenting).
168. *Id*. at 2268.
169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.*

> These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.[173]

Gorsuch also noted that "complete ownership or exclusive control of property" is not likely a necessary condition to the assertion of a Fourth Amendment right, because tenants and resident family members of a home who lack a legal title to the property still have standing to complain about searches of the home they live in.[174] The implication appears to be that a person need not be the sole owner of her or his digital data in order to assert a cognizable right under the Fourth Amendment.[175] Gorsuch concluded his dissent with a lament that litigants like Carpenter had failed to preserve such positive-law-based Fourth Amendment arguments, instead only preserving *Katz*-based arguments.[176]

IV. IMPACT

The law is struggling to keep up with modern technologies. As pointed out in the amicus brief submitted on behalf of a litany of technology conglomerates that included Google, Microsoft, Apple, Twitter, Facebook, and Verizon, "Digital interconnectedness defines modern society."[177] When the Supreme Court decided *Miller* and *Smith* in the 1970s, creating the basis of the third-party doctrine, the Internet did not exist.[178] In the 1970s, third-party disclosure was "rarely necessary" to conduct daily business.[179] Furthermore, when Congress enacted the Stored Communications Act in 1986, few people used the Internet, and only approximately 500,000 Americans subscribed to basic cell-phone service.[180] Today, over ninety-five percent of American adults own cell phones, and seventy-seven percent of those cell phones are smart phones, which people increasingly use as their main means of online

173. *Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J., dissenting).
174. *Id.* at 2269–2760.
175. *See id.*
176. *Id.* at 2272.
177. Brief for Tech. Companies as Amici Curiae in Support of Neither Party at 12, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
178. *Id.* at 13.
179. *Id.*
180. *Id.*

access at home.[181] Smart phones transmit more data in mere minutes than could fit on an entire hard drive in 1986. People now send and receive 269 billion emails worldwide every day.[182] The law has not yet adapted to the digital world.

By virtue of the way the Internet and wireless networks operate, all digital technology transmits user information to various service providers.[183] As Justice Gorsuch asserted, a strict application of *Smith* and *Miller* would yield the logical result that all of this information, shared with third parties, could be reviewed by law enforcement without a warrant.[184] Law enforcement certainly avails itself of this fount of digital information, as well. According to AT&T's 2018 Transparency Report, the company received 121,498 demands for records from the United States government for both civil and criminal proceedings between January 2018 and June 2018 alone.[185] The holding in *Carpenter* is a step toward protecting citizens from such invasive government surveillance without a warrant supported by probable cause, but many sources of digital data lack such safeguards.

A perfect example of contemporary uncertainty regarding the Fourth Amendment's protections of new sources of digital data can be seen in *Arkansas v. Bates*,[186] had consent to the search not been given.[187] In *Bates*, the defendant had several friends over to watch a football game in the evening, and the following morning one of his friends was found dead in his backyard hot tub.[188] Police found several digital "smart" devices in Bates's home, including an Amazon Echo.[189] The tech Goliath initially refused to release the recordings uploaded by the device until Bates himself allowed it.[190] Due to Bates' consent to the search, the scope of Fourth Amendment protection over

181. *Id.*

182. *Id*. at 14.

183. Brief for Tech. Companies as Amici Curiae in Support of Neither Party at 18, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

184. *Id.*

185. AT&T, TRANSPARENCY REPORT (2018), http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport html.

186. Case No. CR-2016-370-2 (Ark. Cir.)

187. Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence From Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM) https://www npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo.

188. *Id.*

189. *Id.*

190. *Id.*

recordings made by digital assistants such as the Amazon Echo remains unadjudicated.[191] Such technologies exemplify the growing "Internet of Things," which is a term for the interconnected network of "smart" devices "used to communicate and process information to an extent that was not possible before."[192] As these "smart" devices continue to become more affordable and ever more ubiquitous, it is only a matter of time before this issue arises again.

The sensitivity of digital data is hardly limited to location information revealed by CSLI.[193] Data generated by new technologies may reveal concerning precious details about the material people read, the precise actions they take on their devices, and more.[194] For example, smartphones often make a record when their users open a news article, view a photograph, or send a message, and those records are then transmitted to third parties such as the operator of the Internet platform or mobile application.[195] These records, which, like CSLI, are created without an additional affirmative act of the user, are not clearly protected. It is not difficult to imagine that it would be desirable for a law enforcement officer to access such records and know what news stories a suspect read, what photos that suspect viewed, and from when and where the suspect sent messages to build up a case. Government agencies could even use this log of data from search engines to show a user's pattern of accessing websites about mental health or substance-abuse treatments. Is this an outcome society is prepared to accept as reasonable?

We are left as a nation to navigate this new reality with a perplexing and contradictory body of precedent from the Supreme Court. *Carpenter's* narrowness does not clearly illuminate the path forward, but digital privacy activists are optimistic about the precedent it has set. American Civil Liberties Union attorney Nathan Freed Wessler said of the decision:

> The government can no longer claim that the mere act of using technology eliminates the Fourth Amendment's protections. Today's decision rightly recognizes the need to protect the highly sensitive

---

191. *Id.*

192. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-570, INTERNET OF THINGS: COMMUNITIES DEPLOY PROJECTS BY COMBINING FEDERAL SUPPORT WITH OTHER FUNDS AND EXPERTISE (2017).

193. Brief for Tech. Companies as Amici Curiae in Support of Neither Party at 31, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

194. Riley v. California, 134 S. Ct. 2473, 2490 (2014).

195. Brief for Tech. Companies as Amici Curiae in Support of Neither Party at 31, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

> location data from our cell phones, but it also provides a path forward for safeguarding other sensitive digital information in future cases—from our emails, smart-home appliances, and technology that is yet to be invented.[196]

So, what does *Carpenter's* holding do? It diminishes, but does not eradicate, the relevance of the third-party doctrine. It also grants citizens more protection from government surveillance in a limited context, which could point the way for further expansions of Fourth Amendment protections of digital data. It offers practitioners strong precedent to argue by analogy that other sources of digital data are just as ubiquitous, revealing, and necessary to modern society, and therefore deserve of the same level of Fourth Amendment protections.

V. CONCLUSION

As our society becomes ever more advanced and exponentially more sources of personal information are digitally created and stored, we must ask ourselves as a nation: what does privacy mean today? As we stand in the midst of an exponential growth in modern technology, the law must advance in step. A strict application of the third-party doctrine would result in none of us having a legitimate privacy interest in almost all our digital data. In our increasingly digital world, this would leave Americans vulnerable to the kind of Orwellian government surveillance the majority was concerned about in *Carpenter.* While *Carpenter* takes a step toward preserving individual privacy, the opinion makes clear that its application is intended to be narrow and does not wholly eradicate the third-party doctrine.

As Gorsuch noted in his dissent, it was the *Katz* reasonableness test that produced the third-party doctrine, which weakened Fourth Amendment protections. However, the *Katz* reasonableness test was employed to strengthen Fourth Amendment protections in *Carpenter*. These seemingly contradictory applications lend credence to criticisms of the test for being circular, amorphous, and overly subjective. Neither the third-party doctrine nor the *Katz* reasonableness test seems adequate in today's digital landscape. A positive-law approach, as suggested by Justice Gorsuch, may successfully marry the Fourth Amendment's roots in property rights with modern society's expectations that privacy be safeguarded from government intrusion. Until Fourth Amendment jurisprudence is further clarified in the broader context of digital data and evolving technologies, it falls upon attorneys to make both positive-

196. *Supreme Court Rules Police Need a Warrant to Track Cellphones*, ACLU (Jun. 22, 2018), https://www.aclu.org/news/supreme-court-rules-police-need-warrant-track-cellphones.

law Fourth Amendment arguments and arguments based on *Carpenter's* reliance on the *Katz* reasonableness test.

*Alexandra Carthew**

*2020 J.D. Candidate at the University of North Dakota School of Law. A special thank you to my mentor, Dane DeKrey, who helped me select this topic, and the rest of the Fargo Federal Public Defender's Office. I will be a better attorney because of your feedback, guidance, and support. Thank you all. I would also like to thank my brilliant friend, Megan Broton, who patiently listened to me discuss this case countless times. Megan, you light up my life. Thank you to my aunt, Chris, for her generous support, love, and biting sense of humor. No expression of my gratitude is complete without mention of my fabulous mother, Laurie. Mom, thank you for your constant love, your inspiring individualism, and never allowing me to take myself too seriously. Finally, a heartfelt thank you to all of my other family members and friends. I am so grateful to you all.