LIBERTY UNIVERSITY

Liberty University Law Review

Volume 14
Issue 1 *Fall 2019*

Article 7

September 2019

Carpenter v. United States: CSLI, Third-Party Doctrine, and Privacy in the Twenty-First Century

William Hopchak

NOTE

CARPENTER V. UNITED STATES: CSLI, THIRD-PARTY DOCTRINE, AND PRIVACY IN THE TWENTY-FIRST CENTURY

William Hopchak

ABSTRACT

Since *Katz v. United States*, Fourth Amendment jurisprudence has revolved around privacy. In *Katz*, the Supreme Court held that the Fourth Amendment protects more than just persons and property but also information in which one has a reasonable expectation of privacy. In *United States v. Miller* and *Smith v. Maryland*, the Supreme Court established the third-party doctrine, which holds that any voluntary communication of information to a third party precludes a reasonable expectation of privacy in that information, and thus, removes it from the protection of the Fourth Amendment. This established paradigm was upset by the Supreme Court's decision in *Carpenter v. United States*.

In *Carpenter*, the appellant challenged the admission of cell-site location information (CSLI) obtained via a subpoena under the Stored Communications Act, on the theory that it was an unconstitutional search requiring a warrant. The Sixth Circuit applied the third-party doctrine to find that since Carpenter voluntarily used his cell phone, effectively disclosing his CSLI to his cellular providers, he had no reasonable expectation of privacy therein. As such, no search within the meaning of the Fourth Amendment occurred, and the evidence was admissible. The Supreme Court reversed. It refused to extend the third-party doctrine to these circumstances and instead drew upon a line of cases suggesting there exists a privacy interest in the totality of one's physical movements.

The Supreme Court's decision rightfully acknowledges the limitations of existing privacy-focused jurisprudence to preserve the spirit if not the letter of the Fourth Amendment in the digital age. The digital revolution has created a unique set of circumstances in which information that in the founding era would be kept in closely held papers is routinely stored on third-party servers. Also, the amount of data that can be passively and constantly generated extends beyond what was conceivable in the not so distant past. These circumstances deeply strain the third-party doctrine's bright line removing all voluntarily conveyed information from the Fourth Amendment's protection. Today, one could quickly face a decision between participation in the modern social and economic world and maintaining any privacy from government search. The Court in *Carpenter* took a small but

significant first step towards reshaping Fourth Amendment jurisprudence to account for new digital realities.

However, the Court also reached its result in a manner likely to create complications in the future. Its reasoning was strained, and did not adequately differentiate this instance from situations where the third-party doctrine precludes Fourth Amendment protection. As a result, courts will have to deal with a still generally applicable third-party doctrine but haunted by the specter that at least sometimes privacy interests are too great to allow the third-party doctrine to operate normally.

This note examines both the desirability of the Court's result, as well as its shortcomings. It then suggests possibly fruitful avenues forward as cases inevitably arise, seeking to restrict the third-party doctrine further and extend Fourth Amendment protections to other types of data. Interestingly, returning to emphasizing property rather than privacy as a deciding factor in Fourth Amendment cases offers significant advantages in simplifying Fourth Amendment jurisprudence, generating useful rules for this area of law in the digital age, and accomplishing privacy centered goals.

I. INTRODUCTION

New technologies and changing circumstances always force the law to develop in order to handle new situations. The digital revolution is in the process of changing daily life in radical ways that courts and legislatures are only beginning to address. Though a difficult and often sluggish process, sometimes the adaptations necessitated by change create opportunities to respond to new challenges while fixing old problems in the law. One such instance is crafting a legal approach to dealing with the copious amounts of data produced through normal daily activities. The Supreme Court ushered in a new era with its decision in *Carpenter v. United States*. The majority found a reasonable expectation of privacy in cell-site location information (CSLI).[1] This was a revolutionary decision for two reasons. First, it suggests that in the future, similar privacy interests might be found in other forms of data generated by an ever-increasing list of daily activities. Second, for the first time, the Fourth Amendment protection was found to be completely removed from property. The CSLI, in which the Court determined Carpenter had a reasonable expectation of privacy protected by the Fourth Amendment, was the property of his cell phone provider. Even though the Court has long held that the Fourth Amendment protects against more than the physical intrusion of property, it has never before given persons a Fourth Amendment interest in the property of another. Before examining in detail the *Carpenter*

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

decision and the opportunities it creates for the simultaneous development of Fourth Amendment jurisprudence and crafting solutions to new big-data related problems, it is necessary to survey the state of Fourth Amendment jurisprudence.

II. BACKGROUND

A. Katz v. United States

For better or worse, privacy has been the nucleus of Fourth Amendment jurisprudence for the last fifty years. In *Katz v. United States*, Katz, the defendant, appealed his conviction for communicating gambling information.[2] FBI agents placed a bug on the outside of the telephone booth Katz used to convey the gambling information.[3] Katz objected to the admission of this evidence at his trial, and the circuit court affirmed the conviction on the grounds that, because "there was no physical entrance into the area occupied by the [the petitioner]," his Fourth Amendment rights had not been violated.[4] Though the Fourth Amendment historically concerned the protection of property, the Supreme Court declared:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[5]

This was the first step in the Court's logic, moving Fourth Amendment jurisprudence beyond a simple property focus. Next, the Court rejected the government's argument that since Katz was plainly viewable inside the glass telephone booth, he was not protected by the Fourth Amendment.[6] The Court stated:

> [A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words

2. Katz v. United States, 389 U.S. 347, 348 (1967).
3. *Id.* at 348.
4. *Id.* at 348–49 (alteration in original) (quoting Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966)).
5. *Id.* at 351 (citations omitted).
6. *Id.* at 352.

> he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[7]

These statements laid the foundation for the shift in Fourth Amendment jurisprudence the Court would accomplish with this case.

The Court went on to dispose of the government's argument that no infringement of Katz's Fourth Amendment rights could have occurred since there was "no physical penetration of the telephone booth from which [Katz] placed his calls."[8] While acknowledging "the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, for that Amendment was thought to limit only searches and seizures of tangible property,"[9] the Court stated, "the premise that property interests control the right of the Government to search and seize has been discredited."[10] The court referenced *Olmstead v. United States*, where the Court decided "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments."[11] The Court used property issues to dispose of the case, deciding that since there was no physical intrusion on the property of the defendant, no search had occurred, even though Olmstead's phone conversations had been surveilled.[12] The Court's rejection of property in *Katz* as the basis of Fourth Amendment analysis radically altered the focus of Fourth Amendment jurisprudence.

Though a rule might be inferred out of the majority decision, the Court did not actually articulate precisely upon what analysis it was deciding; it said simply that the Fourth Amendment protected persons, not places, and that Katz had expected privacy while in the phone booth.[13] In his concurring opinion, Justice Harlan attempted to offer a rule for explanation and future application of the Court's decision. He wrote, "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[14] Applied to *Katz*, Justice Harlan

7. *Katz*, 389 U.S. at 352.
8. *Id.*
9. *Id.* at 352–53.
10. *Id.* at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).
11. Olmstead v. United States., 277 U.S. 438, 455 (1928).
12. *Id.* at 464–65.
13. *Katz*, 389 U.S. at 351–52.
14. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

repeated the majority's opinion that a telephone booth user (subjectively) expects his conversation to be private, and he further opined that such expectation was in fact objectively reasonable.[15] This "reasonable expectation of privacy" test would become a dominant feature of Fourth Amendment jurisprudence moving forward.

B. Terry v. Ohio

One year after *Katz*, in *Terry v. Ohio*, the Full Court adopted Justice Harlan's two-pronged test.[16] In that case, Terry had been arrested after a plainclothes detective observed Terry and two others suspiciously investigating a store front.[17] After arresting them, the detective patted them down and found a revolver in Terry's coat pocket, which was later admitted into evidence.[18] Terry claimed the revolver was inadmissible because the detective had violated his Fourth Amendment rights when he searched his person.[19] The Court saw the central question as being "whether . . . it was reasonable for [the detective] to have interfered with [Terry's] personal security as he did."[20] The Court concluded that such a search was reasonable.[21] The reasonable expectation of privacy test became so ingrained that the Court has even described *Katz* as the "[L]odestar" of Fourth Amendment jurisprudence.[22]

Interestingly, the Court did not at all evaluate the first prong of Justice Harlan's test regarding whether Terry had a subjective expectation of privacy. Perhaps the Court just assumed that there is a universal subjective expectation of privacy as to the contents of one's own pockets. However, the Court has failed to address the first prong so consistently that it has been argued that the subjective expectation of privacy prong of the test has been effectively abandoned.[23]

C. *Third-Party Doctrine*

A key development in Fourth Amendment jurisprudence after the reasonable expectation of privacy test emerged was the third-party doctrine.

---

15. *Id.*
16. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968).
17. *Id.* at 5–7.
18. *Id.* at 7.
19. *Id.* at 7–8.
20. *Id.* at 19.
21. *Id.* at 30–31.
22. Smith v. Maryland, 442 U.S. 735, 739 (1979).
23. Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015).

This doctrine was developed in the cases of *United States v. Miller* and *Smith v. Maryland*.[24] Put succinctly, the third-party doctrine holds that a person has no Fourth Amendment privacy interest in information voluntarily disclosed to a third party.[25]

1. *United States v. Miller*

In *United States v. Miller*, the defendant had been convicted of several charges related to producing whiskey in an unregistered still.[26] Miller had moved for the suppression of his bank records, which detectives obtained with a *subpoena duces tecum*.[27] The district court denied the motion, but on appeal the Fifth Circuit reversed, deciding, "a depositor's Fourth Amendment rights are violated when bank records . . . are obtained by means of a defective subpoena."[28] The Supreme Court, in contrast, found "that [Miller] had no protectable Fourth Amendment interest in the subpoenaed documents."[29]

Miller argued that, "he ha[d] a Fourth Amendment interest in the records kept by the banks because they [were] merely copies of personal records that were made available to the banks for a limited purpose and in which he ha[d] a reasonable expectation of privacy."[30] He argued that the *Katz* reasonable expectation of privacy test protected his banking records from search without a warrant.[31] The Court rejected this argument by also referencing *Katz*, calling attention to the statement "that [w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[32] The Court decided that all records and information Miller revealed to the bank were not protected by a legitimate expectation of privacy, and therefore no Fourth Amendment right was implicated by the government's obtaining the documents via a subpoena.[33]

24. *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435, 436 (1976).

25. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).

26. United States v. Miller, 425 U.S. 435, 436 (1976).

27. *Id.* at 436.

28. *Id.* at 437.

29. *Id.*

30. *Id.* at 442.

31. *Id.*

32. *Miller*, 425 U.S. at 442 (citing Katz, 389 U.S. at 351).

33. *Id.* at 442–43.

2. *Smith v. Maryland*

Three years later in 1979, the Supreme Court decided *Smith v. Maryland*. This case arose from the use of a pen register in a criminal investigation.[34] In response to a request from police investigators, Smith's phone company installed on their property a pen register device that recorded the phone numbers dialed by Smith.[35] Smith was convicted by the trial court, and the Court of Appeals of Maryland affirmed.[36] The Supreme Court took up the case and addressed whether there was a reasonable expectation of privacy in numbers dialed on the phone.[37] Though they maintained that there is an expectation of privacy in the contents of a private phone call, the number dialed was information freely given to the phone company and was not protected by any reasonable expectation of privacy.[38]

These two cases highlight that information freely divulged to a third party is not covered by a reasonable expectation of privacy and is therefore not protected by the Fourth Amendment. This doctrine was relied upon by the Sixth Circuit Court of Appeals in deciding *Carpenter*.[39] It has immense implications in the post-digital revolution setting.

D. *Residual Property Foundations*

Despite the dominance of privacy concerns in twentieth century Fourth Amendment cases, the older property model did not become irrelevant. This is best illustrated in *Florida v. Jardines*. This case concerned "whether using a drug-sniffing dog on a homeowner's porch to investigate the contents of the home is a 'search' within the meaning of the Fourth Amendment."[40] In response to a tip, police took a trained drug dog onto Jardines's porch; the dog alerted for drugs and indicated the strongest source of the smell was the front door.[41] Subsequently, the police obtained a warrant, searched the home, and found marijuana.[42] Jardines was arrested and charged with drug trafficking.[43] Jardines moved for the discovered marijuana plants to be excluded from evidence, claiming that the use of the drug-sniffing dog

34. Smith v. Maryland, 442 U.S. 735, 736–37 (1979).
35. *Id.* at 737.
36. *Id.* at 737–38.
37. *Id.* at 741.
38. *Id.* at 741–42.
39. United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).
40. Florida v. Jardines, 569 U.S. 1, 3 (2013).
41. *Id.* at 3–4.
42. *Id.*
43. *Id.*

violated Fourth Amendment protections.[44] The trial court agreed and excluded evidence found while executing the warrant authorized in response to the canine investigation.[45] The Florida Third District Court of Appeal reversed, but the Florida Supreme Court affirmed the trial court's decision.[46] The Supreme Court "granted certiorari, limited to the question whether the officers' behavior was a search within the meaning of the Fourth Amendment."[47]

Writing for the majority, Justice Scalia began by calling attention to the fact that, originally, Fourth Amendment protections were closely connected to property and physical intrusion thereon by the government.[48] Speaking of *Katz*'s expansion of the Fourth Amendment's scope, Justice Scalia wrote, "though *Katz* may add to the baseline, it does not subtract anything from the Amendment's protections 'when the Government does engage in [a] physical intrusion of a constitutionally protected area.'"[49] Such being the case, Justice Scalia declared *Jardines* to be a simple case: the officers had entered the curtilage of the home and investigated without Jardines's consent.[50] This type of physical intrusion and search is precisely what the Fourth Amendment forbade. Though there is a general, implied license to enter the curtilage of a home to knock on the door, there is no parallel license to bring a trained, drug-sniffing dog to the door to screen for drugs.[51] Justice Scalia also made clear that there was no need to engage in a reasonable expectation of privacy analysis under *Katz*: "One virtue of the Fourth Amendments [sic] property-rights baseline is that it keeps easy cases easy."[52] Since a physical trespass had occurred, the Court decided that Jardines's Fourth Amendment rights had been infringed and affirmed the Florida Supreme Court's decision.[53]

E. *Data Problems*

Such was the legal world in which *Carpenter* arose; however, the actual world had changed significantly since the *Katz*, *Smith*, and *Miller* decisions. The digital revolution has changed and continues to change the world,

44. *Id.* at 4–5.
45. *Id.* at 5.
46. *Jardines*, 569 U.S. at 5.
47. *Id.*
48. *Id.*
49. *Id.* (alteration in original) (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring in judgment)).
50. *Id.* at 5–6.
51. *Id.* at 5–11.
52. *Jardines*, 569 U.S. at 11.
53. *Id.* at 12.

straining a Fourth Amendment jurisprudence that developed in the pre-digital world. The amount of digital data produced is staggering; in 2016 monthly global IP traffic was estimated to reach 91.3 exabytes.[54] Smart phones have become ubiquitous, and the internet of things is looming just on the horizon and will soon be a normal and pervasive facet of life. The internet of things is what the imminent connection and integration of myriad devices, machines, and appliances into the internet is being called. Estimates are that "nearly 26 billion devices [will be] connected to the Internet of Things by 2020."[55]

A great deal of this information will have immense privacy implications. Digital information regarding physical movements, associations, and medical treatments are just a few obvious examples of data with great potential to be highly sensitive. Empirical study indicates that most people are at least somewhat aware of the privacy implications created by big data and disapprove of the pervasiveness of data collection that is currently commonplace on the internet.[56] Even though current law requires disclosure to and consent from users to collect data, most people appear to begrudgingly accept the unwanted invasion of their privacy as the cost of functioning in the digital age.[57] Not only are most people unhappy with how much data the private sector collects, they are "very skeptical of government data collection."[58]

1. Data and Third-Party Doctrine

Sensitive information is vulnerable under the third-party doctrine because it is stored by third parties. Private parties are not restricted by the Fourth Amendment in regards to what data they may collect and record from users, and once that data is given to the third party, or if the data is originally produced by the third party, then the user has no reasonable expectation of privacy in it per *Smith* and *Miller*. This reasoning was displayed in two predecessor cases to *Carpenter*. In *United States v. Davis* and *United States v. Graham*, the courts concluded that CSLI was not protected by the Fourth Amendment because of the third-party doctrine since it was generated and

54. Phil Bradley, *Data, Data Everywhere*, 14 LEGAL INFO. MGMT. 249, 249 (2014) (An "exabyte could hold 100,000 times the printed material in the Library of Congress").

55. *Id.* at 250.

56. Jay P. Kesan, Carol M. Hayes, & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 271 (2016).

57. *Id.*

58. *Id.*

maintained as a business record by the cell service providers, not the cell user.[59]

That the third-party doctrine exposes so much information to government surveillance without requiring demonstration of probable cause and the issuing of a warrant is troubling to scholars and lay people alike. As previously mentioned, the majority of Americans are uncomfortable with governmental surveillance of big data.[60] It is accepted that constitutionally protected rights must cover modern analogs and developments of the right as it existed during the founding era.[61] The issue arises in that much of what was previously kept in one's own records or destroyed is now stored, or even generated, on a third-party server. Strict application of the third-party doctrine renders all such information outside the scope of the Fourth Amendment's protections, but the impact of the digital revolution on daily life may be so significant that protecting what was within the original scope of intent of the Fourth Amendment will require rethinking the protections, or lack thereof, regarding information given to third parties.

In an article in *Brooklyn Law Review*, Amitai Etzioni explains that "[i]n the paper age, the main issue was whether or not the government should be allowed to collect personal information without first gaining a court's approval. . . . [But] [i]n the cyber age, secondary usages of legally-collected information have become so common that a very major concern has become the circumstances under which such usages should be banned to preserve privacy."[62] He continues, "So much legally-collected personal information is available in the hands (or in the cloud) of third parties that their secondary usages determine to a large extent how much privacy we still have."[63]

2. Proposed Solutions

Etzioni believes that a new privacy paradigm is absolutely needed in this digital age because the majority of privacy violations used to be committed by the government directly through primary collection, but now "most violations in the cyber age result from secondary usages of information that has been legally collected."[64] Since the third-party doctrine allows

59. United States v. Graham, 824 F.3d 421 (4th Cir. 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

60. Kesan, *supra* note 56.

61. District of Columbia v. Heller, 554 U.S. 570, 582 (2008) (citations omitted).

62. Amitai Etzioni, *A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational*, 80 BROOK. L. REV. 1263, 1263 (2015).

63. *Id.*

64. *Id.* at 1264.

government to look into any of this legally collected data, Etzioni concludes that:

> [I]f the third party doctrine is allowed to stand, precious little personal information will remain protected from government incursion. Furthermore, because third parties can share information with others and combine it with still more information, the government and corporations can create detailed and intimate dossiers of innocent people unsuspected of crimes. Individuals constantly leave behind a trail of data with every click of a mouse, "data exhaust" akin to the vapors left behind a car.[65]

Etzioni points out that he is not the first to criticize the third-party doctrine in the cyber age.[66] He then propounds a theoretical "Cyber Age Privacy Doctrine" that would evaluate privacy concerns in terms of the volume, sensitivity, and degree of cybernation of the collected material.[67] His model is highly theoretical and in stark contrast to certain well-established points of Fourth Amendment jurisprudence. Though, in fairness to his theory, to depart from established Fourth Amendment jurisprudence is a great deal of his point. However, the model is unlikely to prove workable or adoptable due to its fundamental overhauling of and conflict with established law.

Other scholars have suggested solutions as well. In conjunction with their empirical research on popular opinions regarding big data and government surveillance thereof, Jay P. Kesan, Carol M. Hayes, and Masooda N. Bashir have proposed a clearinghouse model akin to credit score companies: "we suggest the creation of a profile repository to provide a centralized location for consumers to view the nonsensitive information that data brokers and the government hold about them, while also giving consumers the option to

65. *Id.* at 1267.

66. *Id.* at 1267 n.24 (citing Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y. 211, 215 (2006); Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1093 (2006); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564–66 (1990); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, UCLA J.L. & TECH., Spring 2007, at 1, 3; Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1231 (1983)).

67. Etzioni, *supra* note 62, at 1273.

challenge or remove some elements of their profiles."[68] Though perhaps less grandiose than Etzioni's sweeping new paradigm of privacy law, this too appears far from implementable.

Property law, however, has been explored as an avenue that might address the problems created in applying Fourth Amendment jurisprudence to the digital age. Jane Baron explores how the bundle-of-rights metaphor in property law can promote clear thinking and aid in evaluating the competing interests and needs in data.[69] Specifically, Baron explored how different "sticks" could easily be allocated to different parties in the context of electronic health records and privately created consumer databases.[70] If patients and consumers are granted property interests in such data, which currently hover "awkwardly" at the intersection of "existing legal categories such as property, privacy, and intellectual property,"[71] then they would have a Fourth Amendment interest in it and the government would be required to obtain a warrant before accessing the information, even though they would be gaining access via a third party and not via the individual.

III. CARPENTER

A. *Facts*

In *Carpenter v. United States*, the Court addressed "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[72] After a string of robberies in Michigan and Ohio, police arrested four suspects.[73] One of those men implicated the petitioner, Thomas Carpenter.[74] After getting his phone number from the other suspects, prosecutors obtained Carpenter's cell phone records via court orders pursuant to the Stored Communications Act.[75] Federal Magistrates ordered Carpenter's cell service providers "to disclose 'cell/site sector [information] for [Carpenter's] telephone[] at call origination and at call termination for incoming and outgoing calls' during the four-month period when the string of robberies occurred."[76] Such orders were sent to each of

68. Kesan, *supra* note 56, at 272.

69. Jane B. Baron, *Rescuing the Bundle-of-Rights Metaphor in Property Law*, 82 U. CIN. L. REV. 57 (2013).

70. *Id.* at 94–100.

71. *Id.* at 94.

72. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

73. *Id.* at 2212.

74. *Id.*

75. *Id.*

76. *Id.*

Carpenter's providers.[77] The first provider, in response to a demand for 152 days of records, provided records covering 127 days.[78] The second provider, in response to demands for seven days of records, produced two days' worth.[79] "Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[80]

This data was used at trial to show Carpenter was in the area of four of the robberies.[81] Cell phones function by connecting to cell-sites in their proximity.[82] Cell-sites are radio antennas and are usually mounted on towers, though they can also be mounted to myriad smaller objects such as light poles and buildings.[83] Cell-sites generally have multiple directional antennas each covering a particular sector of the covered area.[84] Whenever a cell phone makes a call, it connects to a cell-site; smart phones also connect to the network "several times a minute whenever their signal is on, even if the owner is not using one of the phone's features."[85] "Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)."[86] The denser the concentration of cell-sites in an area, the more precisely the CSLI can be used to locate the phone.[87]

The CSLI data obtained by prosecutors placed Carpenter in the same areas as four of the robberies when they were committed.[88] Carpenter moved for the CSLI data to be excluded at trial, but the district court judge allowed it.[89] In addition to the testimony of seven of his confederates alleging Carpenter was the group's leader, an FBI agent testified as a witness to explain the CSLI data.[90] The agent explained CSLI data and showed a map correlating the CSLI data to the locations of the robberies.[91] Carpenter was convicted of six counts of robbery and five counts of carrying a firearm during a federal crime of violence.[92]

77. *Id.*
78. *Carpenter,* 138 S. Ct. at 2212.
79. *Id.*
80. *Id.*
81. *Id.* at 2212–13.
82. *Id.* at 2211.
83. *Id.*
84. *Carpenter,* 138 S. Ct. at 2211.
85. *Id.*
86. *Id.*
87. *Id.* at 2111–12.
88. *Id.* at 2212–13.
89. *Id.* at 2212.
90. *Carpenter*, 138 S. Ct. at 2212.
91. *Id.* at 2212–13.
92. *Id.*

The Sixth Circuit affirmed the district court's decision, specifically holding that the CSLI data was admissible evidence and applying the third-party doctrine.[93] The Sixth Circuit held "Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers."[94] Since "cell phone users voluntarily convey cell-site data to their carriers as 'a means of establishing communication,' the court concluded that the resulting business records are not entitled to Fourth Amendment protection."[95]

B. *Majority Opinion*

Writing for the majority, Chief Justice Roberts took up the issue of whether the third-party doctrine applied in this instance. Roberts understood the case to "not fit neatly under existing precedents"; it was "at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake."[96] The first line of cases dealt with "a person's expectation of privacy in his physical location and movements."[97] The second line was the above examined reasonable expectation of privacy line of cases.[98]

In handling the first line, Chief Justice Roberts referenced *United States v. Knotts* and *United States v. Jones*.[99] In *Knotts*, investigators used a "beeper" to aid in visually tracking a vehicle to a remote cabin. In that case, "[t]he Court concluded that the 'augment[ed]' visual surveillance did not constitute a search because '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'"[100] In *Jones*, FBI agents used a GPS device to track the petitioner's every driven movement for 28 days.[101] Even though the case was decided on physical trespass grounds, Roberts emphasized that:

> [F]ive Justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. Since GPS monitoring of a vehicle tracks "every movement" a

93. *Id.* at 2213.
94. *Id.*
95. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979)).
96. *Carpenter*, 138 S. Ct. at 2214–15.
97. *Id.* at 2215.
98. *Id.* at 2216.
99. *Id.* at 2215.
100. *Id.* (second and third alterations in original) (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).
101. United States v. Jones, 565 U.S. 400, 403 (2012).

> person makes in that vehicle, the concurring Justices concluded 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.[102]

The spirit of this dicta would figure heavily in the Court's decision in *Carpenter*.

The Court recognized the odd confluence of the two lines of jurisprudence in this one factual situation. CSLI "tracking partakes of many of the qualities of the GPS monitoring we considered in Jones."[103] Chief Justice Roberts continued, "At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle."[104] The Court decided that the third-party doctrine did not extend to Carpenter's "novel circumstances."[105] The Court articulated a new rule:

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to *Fourth Amendment* protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.[106]

The Court thus held that the CSLI data at issue "was the product of a search."[107]

It mattered greatly to the Court that CSLI information was allowing for unprecedented degrees of surveillance. It was more significant to the Court that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," than the fact that new technology had created a situation in which one constantly and voluntarily communicates to a third party his physical location.[108] The situation would be even worse than allowing GPS tracking of vehicles, the Court reasoned,

---

102. *Carpenter,* 138 S. Ct. at 2215 (citations omitted).
103. *Id.* at 2216.
104. *Id.*
105. *Id.* at 2217.
106. *Id.*
107. *Id.*
108. *Carpenter*, 138 S. Ct. at 2217 (alteration in original) (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

since cars are not the constant companion of their owners.[109] The Court referenced studies indicating that most "smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."[110] The third-party exception had been developed in a time when such ease of total surveillance of every physical movement made was inconceivable, and the Court did not believe it so valuable as to require asserting it against expectations of privacy in this new context.

Another point of great concern to the Court was the "retrospective quality of the data."[111] "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection."[112] However, CSLI data is routinely stored by service providers for five years.[113] Thus, any user of any one of the 400 million devices in the country would be subject to government scrutiny of years of their movement.[114] Whenever one finds himself the subject of investigation, it will be as if "he has . . . been tailed every moment of every day for five years."[115]

While the Court was concerned about the retrospective qualities of CSLI data, they were prospective in their ruling. In response to arguments that CSLI data is not granular or specific enough to implicate serious privacy concerns, the Court noted that "CSLI is rapidly approaching GPS-level precision."[116] It is only a matter of time, and probably a short amount of time, before improvements in cellular data and increased volume of cell-site locations will allow CSLI data to precisely locate an individual.

Finally, Chief Justice Roberts briefly asserted that another reason the third-party doctrine does not apply is because CSLI is not voluntarily communicated to the provider.[117] The third-party doctrine extends to voluntarily revealed or communicated information.[118] Chief Justice Roberts wrote that "[CSLI] is not truly 'shared' as one normally understands the

109. *Id.* at 2218.
110. *Id.* (quoting Riley v. California, 573 U.S. 373, 395 (2014)).
111. *Id.*
112. *Id.*
113. *Id.*
114. *Carpenter*, 138 S. Ct. at 2218.
115. *Id.*
116. *Id.* at 2218–19.
117. *Id.* at 2220. Judge Wynn raised this argument in his dissenting opinion in *United States v. Graham*. United States v. Graham, 824 F.3d 421, 442–44 (4th Cir. 2016) (Wynn, Floyd, & Thacker, JJ., dissenting in part and concurring in the judgment).
118. *Id.* at 2219–20.

term."[119] Chief Justice Roberts first asserted, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[120] Next, he noted that CSLI data is created "without any affirmative act on the part of the user beyond powering up."[121] Since just using the phone creates the CSLI, and since using a phone is necessary to participation in modern life, 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."[122]

For these reasons, the Court concluded that "when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[123] It therefore reversed the court of appeals and remanded the case.[124]

C. *Dissenting Opinions*

1. Justice Kennedy

Justice Kennedy authored a dissent in which Justice Thomas and Justice Alito joined.[125] The thrust of Justice Kennedy's argument was that the court should have applied the third-party doctrine.[126] Justice Kennedy phrased the fundamental issue of the case as "whether the Government searched anything of Carpenter's when it used compulsory process to obtain cell-site records from Carpenter's cell phone service providers."[127] He answered this question emphatically in the negative.[128] He asserted that the third-party exception makes clear that one does not have any Fourth Amendment interest in the business records of another.[129] He rejected criticism of *Miller* and *Smith*, stating, "[t]he principle established in *Miller* and *Smith* is correct for two reasons, the first relating to a defendant's attenuated interest in property owned by another, and the second relating to the safeguards inherent in the use of compulsory process."[130] Even though it is now settled that the Fourth

119. *Id.* at 2220.
120. *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
121. *Id.*
122. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).
123. *Id.* at 2219.
124. *Id.* at 2223.
125. *Id.*
126. *Carpenter*, 138 S. Ct. at 2223–24 (Kennedy, J. dissenting).
127. *Id.* at 2226.
128. *Id.*
129. *Id.* at 2226–27.
130. *Id.* at 2227.

Amendment protects persons and their reasonable expectations of privacy, not just property, Justice Kennedy asserted that "the Fourth Amendment's protections must remain tethered to the text of that Amendment, which, again, protects only a person's own 'persons, houses, papers, and effects.'"[131] Essentially, no matter how great the perceived expectation of privacy one may have in the records of another, since those records are not the property of the interested party, the Government has not violated that party's Fourth Amendment rights when it accesses those records. To hold otherwise is to abandon the clear language of the Constitution. Kennedy also asserted that the subpoena procedure required by law is adequate protection.[132]

2. Justice Thomas

Justice Thomas wrote a similar dissenting opinion.[133] He began, "This case should not turn on 'whether' a search occurred. It should turn, instead, on *whose* property was searched."[134] It was, for Justice Thomas, a simple matter. The Fourth Amendment protects "individuals[']. . . right to be secure from unreasonable searches of '*their* persons, houses, papers, and effects.'"[135] Justice Thomas emphasized that the Fourth Amendment protections extend to a parties' own person, houses, papers, and effects, not to the person, houses, papers, and effects of anyone else.[136] Justice Thomas asserted, "[b]y obtaining the cell-site records of [Carpenter's wireless carriers], the Government did not search Carpenter's property."[137] Justice Thomas did not simply claim that the majority made an error applying the reasonable expectation of privacy test; he asserted, "The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence."[138] The thrust of Justice Thomas's argument was that privacy has usurped property as the guiding paradigm for understanding the Fourth Amendment.[139] He asserted that "Justice Harlan's focus on privacy in his concurrence—an opinion that was issued between *Griswold v. Connecticut* and *Roe v. Wade*—reflects privacy's status as the organizing constitutional idea of the 1960s and

131. *Id.*
132. *Carpenter*, 138 S. Ct. at 2228–29.
133. *Id.* at 2235 (Thomas, J., dissenting).
134. *Id.* (citation omitted) (emphasis in the original).
135. *Id.* (emphasis in original).
136. *Id.*
137. *Id.*
138. *Carpenter*, 138 S. Ct. at 2236.
139. *Id.* at 2239–40 (citations omitted).

1970s. The organizing constitutional idea of the founding era, by contrast, was property."[140]

3. Justice Gorsuch

Justice Gorsuch's dissent was unique in that it largely agreed with the result reached by the majority, but it largely disagreed with the reasoning of both the majority and the other dissenting opinions.[141] He was extremely open to finding a means of considering CSLI data to be within the protections of the Fourth Amendment but did "not agree with the Court's decision . . . to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared."[142] He worried that returning to the *Katz* standard "promise[d] more trouble than help."[143] He wanted to explore "more traditional Fourth Amendment approach[es]," and bemoaned the Court's denial of the opportunity to do so by Carpenter's appealing only on the theory of a *Katz's* reasonableness test and failing to preserve other appeals.[144]

a. Critique of third-party doctrine

Justice Gorsuch began by expressing his skepticism that the *Smith* and *Miller* third-party doctrine is well suited to life in the internet age.[145] Since the third-party doctrine excludes from Fourth Amendment protection anything disclosed to a third party and "we use the Internet to do most everything," he wondered "what's left of the Fourth Amendment?"[146] The average American is constantly volunteering information about themselves, and "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."[147] To mechanistically apply *Smith* and *Miller* would mean that "police can review all of this material, on the theory that no one reasonably expects any of it will be kept private."[148] Justice Gorsuch pointed out that "no one believes that, if they ever did."[149] He saw three options for dealing with this situation: "The first is to ignore the problem, maintain *Smith* and *Miller*, and live with the

140. *Id.* at 2240.
141. *Id.* at 2262–2272 (Gorsuch J. dissenting).
142. *Id.* at 2272 (Gorsuch, J., dissenting).
143. *Id.*
144. *Carpenter*, 138 S. Ct. at 2272.
145. *Id.* at 2262.
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*

consequences."[150] Second, the *Katz* reasonableness standard could be applied directly to the situation, and *Smith* and *Miller* could be set aside.[151] Finally, Justice Gorsuch said that an answer could be sought elsewhere outside of the *Katz* paradigm entirely.[152]

(1) Option 1: Continue with *Smith* and *Miller*

Justice Gorsuch rejected the first option of ignoring the problem and continuing with *Smith* and *Miller*.[153] In contrast to the Court's opinion in those cases, "[p]eople often do reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private."[154] He noted that the Supreme Court has never justified the third-party doctrine and instead has simply declared that one who reveals information to a third party "'"assum[es] the risk"' it will be revealed to the police and therefore [there is no] reasonable expectation of privacy."[155] Justice Gorsuch found no convincing justification for this assertion by the Court.[156]

(2) Option 2: Sola *Katz*

Turning to the second option, Justice Gorsuch concluded that even if *Smith* and *Miller* were discarded and the *Katz* test alone were relied upon, problems would remain.[157] First, he agreed that *Katz* is a highly problematic decision and expressed his agreement with the critique of *Katz* offered by Justice Thomas in his dissent.[158] He found it troubling to leave Fourth Amendment protections dependent upon "the breach of some abstract 'expectation of privacy' whose contours are left to the judicial imagination."[159] Justice Gorsuch asserted that "the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period."[160] Moving beyond originalist and historical critiques of *Katz*, Justice Gorsuch argued that "[e]ven taken on its own terms

150. *Carpenter*, 138 S. Ct. at 2262.
151. *Id.*
152. *Id.*
153. *Id.* at 2263.
154. *Id.* (emphasis omitted).
155. *Carpenter*, 138 S. Ct. at 2263 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).
156. *Id.*
157. *Id.* at 2264.
158. *Id.*
159. *Id.*
160. *Id.*

Katz has never been sufficiently justified."[161] He continued, "we still don't even know what its 'reasonable expectation of privacy' test is."[162] He argued that taken either as an empirical question or a normative question, legislators should be defining the reasonable expectation of privacy, not "[p]olitically insulated judges . . . armed with only the attorney's briefs, a few law clerks, and their own idiosyncratic experiences."[163]

(3) Option 3: Pre-*Katz* Property

Finally, Justice Gorsuch turned his attention to traditional, pre-*Katz* Fourth Amendment jurisprudence to see what answers it offered.[164] He did not state precisely what this approach has to offer, but he proposed a clear path forward for future exploration.[165] He called attention to the fact that until the 1960s, "a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the 'reasonableness' of your expectations of privacy."[166] Rather, "it was tied to the law."[167] "The traditional approach asked if a house, a paper or effect was yours under law," and "[n]o more was needed to trigger the Fourth Amendment."[168] Citing *Byrd* and *Jardines*, Justice Gorsuch clarified that this traditional approach has never been discarded, but only overshadowed by *Katz*.[169] Justice Gorsuch observed that due to the dominance of *Katz*, "American courts are pretty rusty at applying the traditional approach to the Fourth Amendment." [170] While it is still clear "that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection," there are things we now do not know.[171] "[W]hat kind of legal interest is sufficient to make something yours? And what source of law determines that? Current positive law? The common law at 1791, extended by analogy to modern times? Both?"[172] Justice Gorsuch believed "[m]uch work is needed to revitalize this area and answer these

161. *Carpenter*, 138 S. Ct. at 2265.
162. *Id.* (emphasis omitted).
163. *Id.*
164. *Id.* at 2267–68
165. *Id.* at 2267–71.
166. *Id.* at 2267.
167. *Carpenter*, 138 S. Ct. at 2267.
168. *Id.* at 2267–68.
169. *Id.* at 2268.
170. *Id.*
171. *Id.*
172. *Id.* (emphasis omitted).

questions."[173] He did not offer to answer those questions in this dissent, but he did offer several points in light of them.[174]

First, Justice Gorsuch called attention to the potential usefulness of bailment law in understanding and articulating a Fourth Amendment jurisprudence for the digital age: "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them," and one does not lose Fourth Amendment protection over bailed property.[175] Justice Gorsuch noted that in some cases the law already recognizes this fact.[176] Mailed letters "are 'as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.'"[177] Justice Gorsuch posited that "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."[178]

Second, Justice Gorsuch pointed out that "complete ownership or exclusive control" is not necessary to vest Fourth Amendment protections.[179] For example, a house may be owned by multiple persons, but each person enjoys Fourth Amendment protections in that home.[180] Further, one who simply resides in a home without any legal title to it still enjoys such Fourth Amendment protections.[181] Having established this premise, Justice Gorsuch posited that "just because you have to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it."[182] He referenced constructive bailments such as are created when one finds lost property.[183] Just as the first owner's property rights, including Fourth Amendment rights, are fully in force over this property that by necessity has come into another's possession, third parties coming into possession of a user's data may not extinguish the user's interests.[184] He noted, "[a]t least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life,

173. *Carpenter*, 138 S. Ct. at 2268.
174. *Id.* at 2268–71.
175. *Id.* at 2268–69.
176. *Id.* at 2269.
177. *Id.* (quoting *Ex Parte* Jackson, 96 U.S. 727, 733 (1877)).
178. *Id.*
179. *Carpenter*, 138 S. Ct. at 2269.
180. *Id.*
181. *Id.* at 2269–70.
182. *Id.* at 2270 (emphasis omitted).
183. *Id.*
184. *Id.*

and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too."[185]

Next, Justice Gorsuch noted that "positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition."[186] He wrote that statutes can create a property interest within the contemplation of the Fifth Amendment's Takings Clause, and that such could be informative for determining what property also enjoys Fourth Amendment protections.[187] Further, "[i]f state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations."[188]

Finally, Justice Gorsuch made the point that "while positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it."[189] His point was that Congress or a state legislature could not enact a law excluding from the Fourth Amendment some sort of property that the Constitution contemplates protecting.[190] Closely related to this was his fifth point that "this constitutional floor may, in some instances, bar efforts to circumvent the Fourth Amendment's protection through the use of subpoenas."[191] Here, Justice Gorsuch noted the intersection of Fifth Amendment and Fourth Amendment principles.[192] He argued that as originally understood, the Fifth Amendment protection from self-incrimination also protected against forced production of incriminating documents.[193] As such, a subpoena should in some cases be viewed as a search or seizure forbidden by the Fourth Amendment, and it should not be allowed to serve as a tool to sidestep Fourth Amendment protections.[194]

Justice Gorsuch ended his dissent on an understated note. He did not seem to take any real issue with the result of the Court's decision; in fact, he spent most of his dissent exploring ways to extend Fourth Amendment protection to data like CSLI. He did fault the Court for deciding "to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered

185. *Carpenter*, 138 S. Ct. at 2270.
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.*
190. *Id.* at 2270–71.
191. *Carpenter*, 138 S. Ct. at 2271.
192. *Id.*
193. *Id.*
194. *Id.*

inquiry."[195] He seemed to believe that, had Carpenter preserved and argued objections grounded in property interests rather than privacy expectations, the case could have been resolved in his favor. Since these points were not argued, they could not be explored, but Justice Gorsuch clearly suggested a willingness and desire to explore these issues in a subsequent case.[196]

III. ANALYSIS

Carpenter is a complicated case dealing with an area of law that was already complicated when it was developed and was made more complicated by the novel strains of the digital age. The situation brings to mind the famous adage: "Hard cases make bad law." The dissenters were right to attack it. The majority's reasoning is strained, but the result the dissents would have preferred does not seem acceptable either. In this case, the majority was clearly working to obtain a specific desirable result, while the dissenters were nobly trying to adhere to sound legal reasoning and defer to precedent. This situation is what makes Justice Gorsuch's dissent so worthy of attention and serious exploration by courts and scholars moving forward.

A. *Strained Reasoning in Majority Decision*

The majority's reasoning is strained. The single greatest example of this, and the one most threatening to their position, is the degree to which they played fast and loose with *Knotts* and *Jones*. The majority attempts to situate the case at the confluence of third-party doctrine and a "reasonable expectation of privacy in the whole of their physical movements."[197] However, its reliance upon *Knotts* and *Jones* is suspect. As Justice Kennedy explained in his dissent, *Knotts* actually asserted that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[198] Justice Kennedy further argued that the "different constitutional principles" which the *Knotts* Court said "may be applicable" in different circumstances only applied when a citizen was subjected to constant surveillance lacking any judicial oversight.[199] Since the CSLI collected in this case was the product of a subpoena obtained from a federal magistrate in conformance with the *Stored Communications Act*, Justice Kennedy believed "[t]hose 'different constitutional principles' mentioned in *Knotts*, whatever they may be, do not

195. *Id.* at 2272.
196. *Id.*
197. *Carpenter*, 138 S. Ct. at 2217.
198. *Id.* at 2231 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
199. *Id.* (quoting *Knotts*, 460 U.S. at 283–84).

apply. . . ."[200] Moving on to address the majority's reliance on *Jones*, Justice Kennedy highlighted the point that the case was decided on property grounds and did not address reasonable expectations of privacy.[201]

B. *Dissent Deficiencies*

However, as strong as this critique of the majority and the others addressed above are, the fact remains that the dissenters failed to seriously consider that what *Knotts* and *Jones* glimpsed may in fact have actually come to pass. The dissenters, while relying upon tighter legal argument and originalist principals, miss a great deal of the point. They would extend old precedent such that the Fourth Amendment would become largely meaningless. What guides the majority is a commitment to the spirit and purpose of the Fourth Amendment. "The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'"[202] The majority reads precedent to indicate that the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power,'" and "that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[203] Commitment to these purposes drove the majority to reach the decision it did.

The dissenters' commitment to the strict property focus of the Fourth Amendment itself is incorrect. Even if the Fourth Amendment is supposed to exclusively protect property—especially the sanctum of the home—how protected can that property be when constantly disclosed data is free for the government's taking? Cellphones are the constant companions of their owners, used inside as well as outside the home. Further, as mentioned before, it will soon be commonplace for many if not all appliances within the home to constantly generate data which is immediately communicated to third parties. Literally, the contents of one's refrigerator would be open to government inspection without any showing of probable cause or obtaining of a warrant. Some strict constructionist originalists will accept this as tolerable since it flows from a straightforward, narrow reading of the text. However, this is in error. The Fourth Amendment protected property in order to protect privacy. Now that technology has changed such that protecting property alone cannot accomplish the same privacy focused goal, accomplishing the spirit of the amendment requires expanding its protection to new realms.

---

200. *Id.* (quoting *Knotts*, 460 U.S. at 284).
201. *Id.*
202. *Id.* at 2213 (quoting Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967)).
203. *Carpenter*, 138 S. Ct. at 2214 (citations omitted).

These same originalists would acknowledge that rights must be understood to adapt with technological development; indeed this is perfectly asserted by Justice Scalia in *District of Columbia v. Heller* where he explains that Second Amendment protections do not extend only to firearms as they existed in the eighteenth century, but to their modern equivalents as well. Justice Scalia wrote, "Just as the First Amendment protects modern forms of communications, . . . and the Fourth Amendment applies to modern forms of search, . . . the Second Amendment extends, prima facie, to all instruments that constitute bearable arms, even those that were not in existence at the time of the founding."[204] Justice Scalia cited *Kyllo v. United States* in making the above point, and the Court in *Carpenter* cited *Kyllo* as well.[205] In *Kyllo*, the Court "rejected . . . a 'mechanical interpretation' of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. . . . [As] any other conclusion would leave homeowners 'at the mercy of advancing technology.'"[206] Possessing the same genius which would animate the *Carpenter* majority, the *Kyllo* Court crafted its ruling in order to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[207]

That the Fourth Amendment should be focused on protecting privacy, and protects property as the means toward that end, is sensible within the broader constitutional context. Given its broad recognition in the American legal landscape, it seems impossible to credibly deny that privacy is a right contemplated by the American legal and constitutional system. Even before the Supreme Court explicitly recognized it, the deep respect for privacy within our Anglo common law tradition manifested in the twentieth century development of common law tort actions for offenses against privacy. Sensing that contemporary pressures required law to recognize a new tort action in response to violations of privacy, Samuel Warren and Louis Brandeis published their seminal *Right to Privacy*.[208] They argued that there existed within the common law tradition a right to privacy the breach of which was compensable. At the root of this right, in their estimation, was "the right to be let alone."[209] Their argument proved timely and convincing.

204. District of Columbia v. Heller, 554 U.S. 570, 582 (2008) (citations omitted).

205. *Id.*; *Carpenter*, 138 S. Ct. at 2214.

206. *Carpenter*, 138 S. Ct. at 2214 (citing Kyllo v. United States, 533 U.S. 27, 35 (2001)).

207. Kyllo v. United States, 533 U.S. 27, 28 (2001).

208. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

209. *Id.*

Prosser, writing in the mid-twentieth century, documented the development of four different common law privacy torts that emerged in response to Warren and Brandeis' argument.[210]

Five years after Prosser's writing, the Supreme Court famously declared the right to privacy to be within the penumbras and emanations of those rights specifically protected in the Constitution.[211] *Katz* drew upon the developing body of law recognizing a right to privacy to explicitly link privacy and Fourth Amendment protections rather than leaving Fourth Amendment protections hanging solely on property interests.[212] While the *Katz* reasonable expectation of privacy standard is susceptible to serious criticism because of the difficulties inherent in applying the test, it seems disingenuous to propose that no right to privacy exists and that it does not have any relationship to Fourth Amendment interests.

Since the Fourth Amendment is concerned with privacy and not just property, it was appropriate for the majority to take the track it did. The modern world has changed what for centuries were normal information storage practices. At the time of the founding, protecting property with the Fourth Amendment also protected privacy. However, that is no longer the case. For the Fourth Amendment to be meaningful at all, it must be understood to protect the sorts of information it was always intended to protect—and not just the old means of storing that information (e.g. the four walls of a home or physical papers). Now that participation in society requires use of technology and that, in using technology, huge amounts of data are constantly disclosed to third parties, existing Fourth Amendment jurisprudence could not be allowed to stand unmodified. It is a simple extension of the principle from *Kyllo* and *Heller* noted above that constitutional protections must progress with technology to protect the modern equivalents of the original object of protection.

In Justice Kennedy's dissent, he objected that the situation in *Carpenter* is no different than the situations in *Miller* and *Smith*.[213] In fact, he argued that CSLI is actually less sensitive than banking and phone records.[214] If this criticism were true, the above argument regarding the need to extend Fourth Amendment protections would be moot. He posited that since "[a] person's movements are not particularly private" because, "[a]s the Court recognized in *Knotts*, when the defendant . . . 'traveled over the public streets he

210. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
211. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
212. Katz v. United States., 389 U.S. 347, 351 (1967).
213. *Carpenter*, 138 S. Ct. at 2231–32.
214. *Id.*

voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination.'"[215] Justice Kennedy reasoned that the location is now even less private since Americans regularly disclose their locations on social media.[216] He also emphasized that, at present, CSLI is not particularly granular and could only be used in Carpenter's case to place his "location within an area covering between around a dozen and several hundred city blocks."[217] Contrary to this, Justice Kennedy noted that phone records and banking records tell with much greater specificity where one goes and with whom he associates.[218] He asserts that these three types of records are all equal in comprehensiveness, retrospectivity, ease of collecting, and voluntariness.[219] It is not certain that this is the case for all elements however. In terms of their retrospectivity, ease of collection, and voluntariness, CSLI, phone records, and bank records are probably equivalent. However, CSLI is at least potentially more comprehensive than phone and financial records. While those documents can present quite comprehensive pictures of certain activities, CSLI data creates a comprehensive record of one's physical movements. As previously discussed, *Knotts* and *Jones* recognize that privacy begins to be implicated when the totality of one's physical movements are recorded.[220] Bank records could also feasibly be used to create a rather complete picture of one's physical movements—assuming one spends money via check, debit card, or credit card regularly as he moves about. However, while "it is impossible to participate in the economic life of contemporary society without maintaining a bank account," it is not necessary to spend money in such a manner as to create a record of one's physical movements.[221] This is different from cell phones, which are a necessary part of modern life and cannot be reasonably used in a manner that does not produce CSLI.

This again raises the issue of whether bank and phone records are any more voluntarily created than CSLI. Insofar as one voluntarily chooses to create any of these types of records by using the various services and products, the answer is no. However, in that neither phone records nor bank records need create a comprehensive picture of one's physical movements, and cell phones cannot be used in a manner that does not create such a

215. *Id.* at 2232 (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).
216. *Id.*
217. *Id.*
218. *Id.*
219. *Carpenter*, 138 S. Ct. at 2232.
220. *See supra* III. B.
221. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

picture, the disclosure of CSLI data is far less voluntary than the disclosure of bank and phone records.

So, not only ought the Fourth Amendment protections be adapted and extended to protect the original object of the Fourth Amendment, it is simply not tenable to maintain that CSLI data presents no new strains on existing jurisprudence requiring modification. The majority was right to remain focused on the fundamental purpose of the Fourth Amendment and perceive the threats created by the digital revolution. However, the dissenters on the whole do have a point. First, the *Katz* test is deeply flawed, and any derivative rule therefrom can be expected to share in its unwieldiness. Second, *Carpenter* has upset existing law and will require an incredible amount of development and clarification. Having extended Fourth Amendment protections to the property of another for the first time, but refusing to articulate a general rule beyond CSLI, chaos can be expected as the circuit courts seek ways to apply this allegedly limited precedent to the cases that will inevitably follow. These problems are why Justice Gorsuch's dissent cannot be ignored and should be the focus of much study moving forward.

Justice Gorsuch was the only dissenting Justice who seemed to appreciate the object of the majority even though he could not bring himself to join it. He stated that he could not "fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong."[222] Noting that the Sixth Circuit had been bound by precedent to apply the third-party doctrine, he affirmed that "this Court can and should" reject it.[223] Justice Gorsuch thus manifested himself as the only dissenter sensitive to the majority's driving purpose of protecting privacy interests within the original object of the Fourth Amendment.

Justice Gorsuch did not join with the majority, however, because rather than leaving "*Smith* and *Miller* on life support and supplement[ing] them with a new and multilayered inquiry," Justice Gorsuch wanted a return to pre-*Katz* jurisprudence.[224] As previously explored, Justice Gorsuch saw great opportunity for satisfactorily protecting Fourth Amendment privacy interests in data via property law. This emphasis upon property law as a means forward has the distinct advantage of allowing for fully protecting the privacy that is the entire point of the Fourth Amendment while staying clearly within the original letter of the Constitution. Simply extending Fourth Amendment interests to the property of others should probably be done if absolutely necessary in this new digital world to accomplish the purpose of the Fourth Amendment, but accomplishing the same purpose without such

222. *Carpenter*, 138 S. Ct. at 2272.
223. *Id.*
224. *Id.*

innovation is preferable. The fact that the *Katz* Court may have discovered and recognized situations where, in order to accomplish Fourth Amendment purposes, one need not have a corresponding property interest, does not mean that solving all subsequent hard problems will require some similar innovation.

Statutorily created property interests in data probably present the best path forward. As is regularly stressed in criticism of *Katz*'s reasonable expectation of privacy, judges are poorly situated to make policy decisions about such issues. Legislatures are best situated to make decisions about what should and should not be private and could grant property interests in user-generated data sufficient to create Fourth Amendment interests in that data.

As Justice Gorsuch notes, positive law cannot be permitted to undercut a person's Fourth Amendment right.[225] He illustrates the point saying, "[l]egislatures cannot pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause."[226] However, while the Constitution provides a floor beneath which one's Fourth Amendment rights cannot fall, it is perfectly possible to create new property interests that extend Fourth Amendment protections.

Justice Gorsuch appropriately sought to maintain the object of the Fourth Amendment and perceived the deficiencies of prior precedent to function in the digital age. However, he did not want to support a weak and flawed approach to solving the problem. His property suggestion offers the advantage of creating bright line, constitutionally orthodox tests for protecting the privacy of Americans in the digital age.

IV. CONCLUSION

The *Carpenter* decision was a first step by the Supreme Court to address the incredible strains placed upon Fourth Amendment jurisprudence by the digital revolution. While the majority rightfully prioritized the spirit over the letter of the Fourth Amendment and crafted a decision to maintain privacy, its decision was strained and is still wed to the *Katz* reasonable expectation of privacy test with all its faults. Indubitably, many more similar cases will begin to flood the Courts in the immediate future. It remains to be seen if the Court will keep stretching and improvising solutions within the *Katz* paradigm and in line with the recent *Carpenter* decision, or if the avenues Justice Gorsuch proposed for simpler, more robust, and sounder solutions to these problems will be substituted.

225. *Id.* at 2270.
226. *Id.* at 2270–71.