THE QUALITATIVE FOURTH AMENDMENT: THE CASE FOR A REFINED, INFORMATION-FOCUSED APPROACH TO FOURTH AMENDMENT CASES INVOLVING NONTRESPASSORY GOVERNMENT SURVEILLANCE

TABLE OF CONTENTS

INTRODUCTION 1728
I. THE RELEVANT HISTORY OF FOURTH AMENDMENT DOCTRINE 1731
A. Katz *and the "Reasonable Expectation of Privacy"* 1732
B. Ciraolo, Riley, *and Public Exposure* 1733
C. Recent Cases Involving Modern Technology 1735
D. Carpenter v. United States *in Context* 1737
1. The Facts of the Case 1738
2. The Court's Holding 1739
II. FINDING A THROUGH LINE IN FOURTH AMENDMENT DOCTRINE 1741
A. The Many Unsatisfactory Candidates 1742
B. An Effective Information-Based Approach 1747
*1. The Obtainable Information Approach as a Through Line for Post-*Katz *Fourth Amendment Cases* 1747
2. The Information-Based Approach as a Roadmap for the Future 1749
a. The Continuing Relevance of the Trespass Qualification 1750
b. Defining "Surveillance Technology" 1750
III. THE THORNY THIRD-PARTY DOCTRINE 1753
A. The Smith-Miller *Standard* 1754
B. Carpenter *and Third-Party Doctrine* 1756
C. Third-Party Doctrine and the Obtainable Information Standard 1758
CONCLUSION 1760

INTRODUCTION

In his 2001 majority opinion for *Kyllo v. United States*, Justice Scalia adopted his characteristic chiding tone to gently reproach what he saw as a notably liberal departure from the original textual interpretation of the Constitution.[1] The *Katz* test for Fourth Amendment violations,[2] to Scalia, was plainly "circular, and hence subjective and unpredictable."[3] That it was one of the most influential and oft-discussed decisions the Supreme Court has ever handed down[4] made little difference; regardless of whatever Justice Harlan and his successors had said, the Fourth Amendment was, at its heart, a protection against government interference with property and had never been tied to "the quality or quantity of information obtained."[5]

Of course, Scalia's property-centric reproach of *Katz*'s legacy was far from unprecedented. In fact, legal scholars as well respected as Judge Richard Posner of the Seventh Circuit Court of Appeals had been slinging the very same criticisms at the two-prong *Katz* test for years.[6] No matter one's opinion of either of these jurists, or of the ubiquitous "reasonable expectation of privacy"[7] test, it would be difficult to argue that it has been easy to apply in practice. And the Court has, frustratingly, avoided directly addressing the issue.[8] Given this, one might be tempted to join the textualists in their

1. 533 U.S. 27, 31-40 (2001).

2. *See* Katz v. United States, 389 U.S. 347 (1967).

3. *Kyllo*, 533 U.S. at 34.

4. *See* THE SOCIAL HISTORY OF CRIME AND PUNISHMENT IN AMERICA 578 (Wilbur R. Miller ed., 2012) (noting the influence of the *Katz* decision).

5. *See Kyllo*, 533 U.S. at 37.

6. *See* Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 ("[I]t is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is."). *But see generally* Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1747 (2017) ("[P]opular privacy expectations are far more stable than most judges and commentators have been assuming.").

7. *See Katz*, 389 U.S. at 360 (Harlan, J., concurring).

8. Orin Kerr, *Answering Justice Alito's Question: What Makes an Expectation of Privacy 'Reasonable'?*, WASH. POST (May 28, 2014, 8:50 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/28/answering-justice-alitos-question-what-makes-an-expectation-of-privacy-reasonable/ [https://perma.cc/D9NR-KZAE].

opinion that the old, easy-to-apply, property-based standard is superior.

That does not mean, however, that the *Katz* test has led to undesirable outcomes. In the age of modern technology, when the government has access to surveillance methods allowing unprecedented intrusion into the privacies of life,[9] Americans are more conscious of their privacy interests than ever and less confident that those interests will be protected.[10] For all the valid criticisms that may be levied against it, the *Katz* test, at the very least, offers an avenue for confronting these concerns.

This is exactly what happened when the Court rendered its decision in *Carpenter v. United States*, a landmark case extending Fourth Amendment protection to historical cell site location information (CSLI)—data generated, collected, and maintained by cell phone service providers entirely outside the control of the individuals the data describes.[11] Reactions to *Carpenter* varied,[12] but it should be clear to anyone who understands the history and context behind the Court's decision that it represents a direct repudiation of the notion that the appropriate Fourth Amendment analysis is not "tied to measurement of the quality or quantity of information obtained."[13] In fact, the *Carpenter* analysis was explicitly tied to both the quantity *and* quality of the information at stake.[14]

---

9. *See Surveillance Technologies*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies [https://perma.cc/B7FW-S5HF].

10. Over 90 percent of American adults say that controlling what information is collected about them and who collects it is important to them, but only 6 percent are "very confident" that government agencies can keep their records private. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RSCH. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/V2DD-FSXY].

11. 138 S. Ct. 2206 (2018).

12. *Compare* Vania Mia Chaker, *Your Spying Smartphone: Individual Privacy Is Narrowly Strengthened in* Carpenter v. United States*, the U.S. Supreme Court's Most Recent Fourth Amendment Ruling*, 22 J. TECH. L. & POL'Y 1, 16 (2018) (arguing that the risk of intrusive government surveillance "may militate in favor of strengthened judicial oversight"), *with* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 944, 950 (2019) (arguing that the categorical warrant requirement was a mistake, and that *Carpenter* should be interpreted narrowly).

13. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001).

14. *See Carpenter*, 138 S. Ct. at 2223 (deciding based on the "depth, breadth, and comprehensive reach" of CSLI).

But the problem remains unaddressed, as the Court has yet to outline an all-encompassing approach to Fourth Amendment cases of unwarranted government surveillance that do not involve physical trespass.[15] These kinds of cases rarely overrule each other, so it seems intuitive that the Court should be able to establish some consistent through line. Yet, so far, it has not. This Note proposes that it can be done, but only if the Court readily admits that the Fourth Amendment no longer protects only property, but also information. The ultimate outcome of *Carpenter*, and of every case that has adequately applied the *Katz* test, has been to keep certain information out of government hands.

Somewhat ironically, this includes *Kyllo*. It is from the language of *Kyllo*, originally intended to protect the traditionally privileged space of the home,[16] that this Note draws inspiration for its proposed rule: absent probable cause, the Fourth Amendment proscribes the government from obtaining information that could not otherwise have been obtained without resorting to surveillance technology or physically trespassing on private property. This relatively simple standard, which can be called the obtainable information rule, unifies the collective holdings of post-*Katz* surveillance cases and provides a flexible framework for future decisions and new technologies.

In order to understand exactly how the obtainable information standard works, it is important to place it in the historical context of Fourth Amendment doctrine. Part I of this Note will examine the history of Fourth Amendment doctrine in cases of government surveillance since 1967 and leading up to *Carpenter v. United States*, a landmark case of critical importance to this argument. Part II will explore some of the theories proposed by academics for reconstructing, clarifying, or otherwise refining Fourth Amendment surveillance doctrine in a palatable manner, and will explain why each is unsatisfactory in at least one regard. It will then formally

---

15. Cases of government surveillance that do involve trespass are, of course, much easier to resolve. It is widely accepted that the Fourth Amendment, at a minimum, prevents the government from physically searching your home or interfering with your personal effects without a warrant. *See Kyllo*, 533 U.S. at 31. This understanding is what allowed *United States v. Jones* to be resolved unanimously, despite the Court's deep divide over the issue of GPS surveillance. *See infra* notes 53-59 and accompanying text.

16. *See Kyllo*, 533 U.S. at 34.

propose the obtainable information standard as a satisfactory alternative, capable of unifying post-*Katz* surveillance jurisprudence under a single theory. Part III will discuss the intersection between the obtainable information standard and third-party doctrine, which has become a subject of much discussion (and concern) following *Carpenter*. It will explain how the third-party doctrine need not be thrown out the window in order to accommodate the proposed standard.

Finally, it is worth noting that the purpose of this Note is not to argue that the obtainable information rule is the solution most resonant with the original meaning of the Fourth Amendment. Rather, the primary purpose of the rule is to synthesize the various holdings of the Supreme Court since *Katz* into a single, easy-to-apply standard. As Part II will explain, there is also good reason to believe that it is the most functionally desirable rule, but this Note does not address the contention that any or all of the Supreme Court's holdings since *Katz* were themselves unconstitutional and should be overruled.

I. THE RELEVANT HISTORY OF FOURTH AMENDMENT DOCTRINE

In the first half of the twentieth century, the Supreme Court had consistently taken a physical property-based approach to assessing Fourth Amendment claims.[17] Perhaps the most notable example of this approach was Chief Justice Taft's declaration in *Olmstead v. United States* that the Fourth Amendment should be construed narrowly enough to apply only to "material things—the person, the house, his papers or his effects."[18] The Taft Court ultimately held that warrantless wiretapping did not violate the Fourth Amendment, as there was no actual physical entry of the defendant's house or seizure of his belongings.[19] Following *Olmstead*, the Court continued to apply this narrow construction of the Fourth Amendment,

17. The Fourth Amendment protects "persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV.

18. 277 U.S. 438, 464 (1928).

19. *Id.* at 466.

finding violations only when the government had physically intruded upon a defendant's property.[20]

A. Katz *and the "Reasonable Expectation of Privacy"*

Then, in 1967, the Court dramatically expanded the realm of Fourth Amendment doctrine with its opinion in *Katz v. United States*.[21] Charles Katz was convicted of transmitting wagering information via telephone based on evidence gathered from warrantless FBI recordings of his phone conversations.[22] The district and appeals courts quickly rejected his Fourth Amendment claims because the agents never actually intruded on any property Katz owned.[23] However, in a landmark decision, the Supreme Court overruled *Olmstead*, rejecting the constitutional requirement of physical trespass or seizure.[24] Moreover, the Court took a step further and declared that "the Fourth Amendment protects people, not places,"[25] effectively ending the era of the property-based approach.[26]

The majority opinion in *Katz* offered no clear standard for courts to utilize when assessing Fourth Amendment claims, but Justice Harlan's concurring opinion proposed a two-step test: (1) that the defendant exhibited a subjective expectation of privacy, and (2) that the expectation is "one that society is prepared to recognize as reasonable."[27] Twelve years later, in *Smith v. Maryland*, a majority of the Court adopted Harlan's "reasonable expectation" test, and a new era of Fourth Amendment jurisprudence was born.[28]

All was not said and done, however. *Katz*'s new interpretation of the rights protected against unreasonable search and seizure created a slew of new questions, especially as technology continued to

---

20. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 510-12 (1961); Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2018 CATO SUP. CT. REV. 79, 83.

21. 389 U.S. 347 (1967).

22. *Id.* at 353.

23. *Id.* at 348-49.

24. *Id.* at 353.

25. *Id.* at 351.

26. *See* Burrus & Knight, *supra* note 20, at 83.

27. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted).

28. 442 U.S. 735, 740 (1979).

rapidly advance near the beginning of the twenty-first century. Foreseeing the danger that advancing technology poses to sources of constitutionally protected private activity, the Supreme Court chose to sharpen the focus of *Katz* while simultaneously reintroducing a traditional spatial context to the analysis.[29]

B. Ciraolo*,* Riley*, and Public Exposure*

A key qualification of the Court's opinion in *Katz* was the idea of public exposure: anything that has been "knowingly expose[d] to the public" cannot reasonably be expected to be kept private.[30] This would seem self-evident and perhaps more relevant to the first prong of the *Katz* test. After all, if Charles Katz had shouted the details of his criminal enterprise across a crowded room, he could hardly have claimed any subjective expectation that his words would remain private. However, the concept of "public exposure" has taken up a more permanent home in the second prong of the *Katz* test, which the Court has used to prevent unsuccessful attempts to conceal criminal activity from creating constitutionally protected interests.

This is exactly what happened in 1986, when the Court upheld the conviction of Dante Ciraolo.[31] Law enforcement had been tipped off that Ciraolo was growing marijuana in his yard but were unable to confirm their suspicion from ground level due to the ten-foot fence enclosing his property.[32] Without a search warrant, the police opted instead to fly over Mr. Ciraolo's property and surveil his yard from a private airplane.[33] The officers identified multiple marijuana plants and obtained a search warrant for that evidence.[34]

The Supreme Court fully acknowledged Mr. Ciraolo's subjective expectation of privacy, exhibited by his efforts to conceal his yard

---

29. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 588 (2017). For more on the context and reasoning behind the *Kyllo* decision, see generally David A. Sklansky, *Back to the Future:* Kyllo*,* Katz*, and Common Law*, 72 MISS. L.J. 143 (2002).

30. *Katz*, 389 U.S. at 351.

31. California v. Ciraolo, 476 U.S. 207, 210 (1986).

32. *Id.* at 209.

33. *Id.*

34. *Id.*

from prying eyes.[35] However, even an intent "to conceal assertedly private activity" is meaningless in cases of public exposure.[36] According to the Court, the determinative fact was that any person flying in publicly navigable airspace on a commercial flight or private airplane could have "glanced down" and seen exactly the same thing that the officers saw.[37] In other words, exposure to the public is a hard line drawn when an effect or activity is located in a space that could theoretically be observed from a public vantage point, whether or not it actually was observed.

The Court affirmed as much in *Florida v. Riley*, a similar case involving police use of a helicopter to surveil the interior of a dilapidated greenhouse from four hundred feet above.[38] The plurality opinion upheld the conviction largely based on the fact that the helicopter never left public airspace as defined by FAA regulations, meaning any person in a helicopter could have lawfully made the same observations.[39] Justice O'Connor's concurring opinion was hesitant to rely on such regulations, but would have instead inquired whether members of the public travel in helicopters at that altitude "with sufficient regularity" so as to render any expectation of privacy unreasonable.[40] In any case, Riley's conviction was upheld because the marijuana he was growing in his greenhouse had been exposed to the public in the sense that any member of the public could presumably have made such an observation without breaking any laws or acting in an irregular manner.[41] Mr. Riley's subjective expectation that his greenhouse would remain private, and the fact that no member of the public (other than police officers) subverted that expectation, were found to be inconsequential.[42]

What arose from these cases was a definitive limit on the scope of the *Katz* test—and perhaps a necessary one given its potential nebulousness. The Court effectively used the "public exposure"

35. *Id.* at 211.

36. *Id.* at 212 (internal quotation marks omitted) (quoting Oliver v. United States, 466 U.S. 170, 181-83 (1984)).

37. *Id.* at 213-14.

38. *See* 488 U.S. 445, 448 (1989).

39. *Id.* at 450-51.

40. *Id.* at 454 (O'Connor, J., concurring).

41. *Id.* at 450-51 (plurality opinion).

42. *See id.* at 451.

exception to narrow *Katz*'s "reasonable expectation" prong so as to apply only to effects and activity which had been kept completely private from all potential public observation.[43] Along with the open fields doctrine[44] and the third-party doctrine, which will be discussed later in this Note,[45] *Ciraolo* and *Riley* demonstrate the Court's willingness in the late 1980s to poke holes in personal expectations of privacy using theoretical societal reasonableness.

C. Recent Cases Involving Modern Technology

By the dawn of the twenty-first century, it became clear that such legal hole-poking posed a serious threat to traditional constitutionally protected spaces. In *Kyllo v. United States*, the Court considered the warrantless use of a thermal imaging device to detect heat signatures emanating from a suspect's home.[46] The Court rejected the government's argument that these heat waves were not subject to a reasonable expectation of privacy, finding instead that any technology that obtained "information regarding the interior of the home that could not otherwise have been obtained without physical intrusion" constituted a search.[47] This line of reasoning allowed the Court to emphasize the continued relevance of constitutionally protected spaces under the Fourth Amendment (such as homes) while simultaneously preserving the underlying *Katz* objective of

---

43. This principle is perhaps best illuminated by the Supreme Court's 1984 decision in *Karo v. United States*, 468 U.S. 705 (1984). In *Karo*, the Court held that the use of a surreptitiously placed electronic tracking beeper to monitor the movement of a five-gallon can of chemicals purchased by a suspected criminal violated the Fourth Amendment. *Id.* at 714. What made this decision particularly remarkable was the Court's decision in *United States v. Knotts* only one year before, a case involving the use of a similar tracking beeper placed in a can of chemicals, in which the Court held that there was *not* a Fourth Amendment violation. 460 U.S. 276, 285 (1983). The distinction, as explained by Justice White in the *Karo* majority opinion, came down to the potential for simple "visual surveillance." *See Karo*, 468 U.S. at 714. In *Knotts*, law enforcement had used the beeper to track the defendant along public thoroughfares to the area where his cabin was located, activity that might just as well "have been observed by the naked eye." *Id.* at 713-14. In *Karo*, on the other hand, the beeper was used to track movement within a private home, a place "not open to visual surveillance." *Id.* at 714.

44. *See generally* Oliver v. United States, 466 U.S. 170 (1984); United States v. Dunn, 480 U.S. 294 (1987).

45. *See infra* Part III.

46. 533 U.S. 27, 29-30 (2001).

47. *Id.* at 34 (internal quotation marks omitted).

not "leav[ing] the homeowner at the mercy of advancing technology."[48] Critically, the Court rejected the "proposition that inference insulates a search"; that is, simply because the officers had to infer additional conclusions from the heat data gathered did not make the data any less private.[49]

Justice Scalia's majority opinion in *Kyllo* is plainly critical of the *Katz* test, or at least of the way in which it is worded. Before even attempting to apply it, Scalia uses the words "circular," "subjective," and "unpredictable" to describe the "expectation of privacy that society is prepared to recognize as reasonable."[50] This problem springs from the fact that, in Scalia's opinion, the Fourth Amendment "has never been tied to ... the quality or quantity of information obtained."[51] The government's use of thermal imaging was unconstitutional not because the actual activity observed was private in nature but because activity that takes place within the walls of the home is necessarily protected by the Fourth Amendment.[52] In many ways, this can be seen as an attempt to refocus the Court's Fourth Amendment doctrine on specific constitutionally protected areas—what might be called a property-based approach.

A decade after *Kyllo*, the Supreme Court ruled on another landmark Fourth Amendment case, *United States v. Jones*.[53] Jones argued that the government's warrantless use of location data gathered from a GPS device planted on his car constituted an unreasonable search.[54] The Court ultimately ruled in favor of Jones, although on admittedly mixed grounds.[55] Once again, Justice Scalia wrote the majority opinion, taking the traditional approach and arguing that the defendant's rights were violated when the officers "physically occupied private property for the purposes of obtaining information."[56] Justice Alito, joined by three other Justices, concurred in the judgment but explicitly rejected

48. *Id.* at 35.
49. *Id.* at 36.
50. *Id.* at 34.
51. *Id.* at 37.
52. *See id.* at 34.
53. 565 U.S. 400 (2012).
54. *Id.* at 402-03.
55. *See id.* at 413.
56. *Id.* at 404.

the majority's pre-*Katz* approach.[57] Instead, Alito argued that the long-term use of GPS monitoring to track a person's precise movement impinges on that person's reasonable expectation of privacy.[58] Justice Sotomayor was the lone voice in agreement with both Scalia and Alito.[59] As such, a five-member majority of the Court agreed that the precise details of a person's location over a period of time are subject to a "reasonable expectation of privacy" and therefore deserving of Fourth Amendment protection.

The Court offered a more unified perspective in 2014 when it considered the much-discussed case of *Riley v. California*.[60] The issue in *Riley* was narrower than that in previous cases: merely the ability of the government to search, without a warrant, data on a cell phone recovered from a person during a lawful arrest.[61] However, the implications were no less important. The Court held that, unlike other objects that might be kept on an arrestee's person, "[c]ell phones differ in both a quantitative and a qualitative sense."[62] Unlike a wallet or paper document, modern cell phones can hold vast quantities of personal images, private communications, and personal information that "is not physically limited in the same way."[63] The Court reasoned that to allow unwarranted searches of such information would be to allow unreasonable government intrusion into "the privacies of life."[64] Interestingly, the majority made no mention of *Katz* in its opinion, despite the clear connection.

D. Carpenter v. United States *in Context*

Carpenter, therefore, was only the most recent in a long line of cases since *Katz* cyclically broadening and refining the scope of

---

57. *Id.* at 426 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.").

58. *Id.* at 430.

59. *See id.* at 414 (Sotomayor, J., concurring) ("When the government physically invades personal property to gather information, a search occurs.... Nonetheless, as Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance.").

60. 573 U.S. 373 (2014).

61. *See id.* at 378.

62. *Id.* at 393.

63. *Id.* at 394.

64. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

Fourth Amendment protection; it was against this background that the Court rendered its decision. And while some scholars heralded the Court's holding in *Carpenter* as revolutionary,[65] others wondered why it took the Court so long.[66] Whatever the case, it should be noted that the key concerns about the government's access to private information, made possible by technological advances discussed in *Jones* and *Riley v. California*, underpin the outcome of *Carpenter*.[67] The same could be said about the technological equivalence principle adopted in *Kyllo*.[68] This makes *Carpenter* the latest installment in a trilogy (or perhaps a tetralogy?) of decisions confronting the interplay between the Fourth Amendment and continuously advancing surveillance technology.[69] For these reasons, it is important to keep context in mind when considering *Carpenter*.

1. The Facts of the Case

Over a period of four months in 2011, a group of armed men robbed a series of Radio Shack and T-Mobile stores in Detroit.[70] Police officers arrested four men in connection with the robberies, one of whom admitted to participating in the crime spree and provided the names and phone numbers of fifteen accomplices.[71] Using this information, prosecutors procured court orders under the Stored Communications Act compelling two wireless carriers to disclose cell site location information (CSLI) data for several suspects, including Timothy Carpenter.[72]

---

65. *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) ("*Carpenter* works a series of revolutions in Fourth Amendment law.").

66. *See, e.g.*, Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 231-32 (2018) (arguing that "it is sobering to consider" how long it took the Court to correct "a widespread error that enabled constitutional violations on an epic scale").

67. Chaker, *supra* note 12, at 7-8.

68. *See* Ohm, *supra* note 65, at 394-95.

69. *See* Freiwald & Smith, *supra* note 66, at 216.

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

71. *Id.*

72. *Id.*

CSLI is, in essence, all the information that cell phones relay to the nearby cell towers.[73] Wireless carriers routinely store customers' historical CSLI, which can triangulate a cell phone's location at any given time.[74] The Stored Communications Act, originally enacted in 1986 as Title II of the Electronic Communications Privacy Act, permits disclosure of such data upon a showing of "reasonable grounds to believe" that it is "relevant and material to an ongoing criminal investigation."[75] Of course, this standard is notably lower than that required to obtain a warrant, which requires probable cause.[76]

Altogether, the government procured 12,898 location points cataloguing Carpenter's movements over a period of four months.[77] Before trial, Carpenter moved to suppress the CSLI, but the district court denied his motion.[78] At trial, the government used the CSLI to place Carpenter's phone near four of the robberies.[79] Based largely on this evidence, Carpenter was convicted of all but one of the charges and sentenced to more than one hundred years in prison.[80] The Sixth Circuit Court of Appeals affirmed the conviction, and the United States Supreme Court granted certiorari to resolve a circuit court split on the issue.[81]

2. The Court's Holding

The opinion of the Court, authored by Chief Justice Roberts, began its analysis by reaffirming the Court's commitment to upholding the "reasonable expectation of privacy" standard adopted in *Katz*.[82] However, the Court chose to go more in-depth by using a multifactor analysis which, although not explicitly listed in the

73. Stephanie Lacambra, *Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys*, ELEC. FRONTIER FOUND. (Oct. 30, 2017), https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf [https://perma.cc/M2MD-R6D6].

74. *Id.*

75. 18 U.S.C. § 2703(d).

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

77. *Id.* at 2212.

78. *Id.*

79. *Id.* at 2212-13.

80. *Id.* at 2213.

81. *Id.*

82. *See id.*

opinion, was central to the holding.[83] While each of these factors, including duration, scope, and intrusiveness, informed the Court's ultimate decision, none were dispositive on their own.[84] It was, at its heart, a balancing test—much to the chagrin of the dissenters.[85]

In sum, the Court found that by acquiring his CSLI, the government impinged Carpenter's reasonable expectation of privacy and therefore committed a search under the meaning of the Fourth Amendment.[86] *Katz* and *Jones* taken together, according to the Court, stood for the proposition that people can maintain a reasonable expectation of privacy in their activities even when those activities are performed outside the sanctuary of their home.[87] Likewise, *Riley v. California* and *Kyllo* addressed the need for Fourth Amendment doctrine to grow and change in proportion to the changing nature of technology.[88] Therefore, even an interpretation of the Constitution that demanded "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" requires a somewhat flexible approach.[89]

The Court cited the five-Justice majority in *Jones* for the proposition that society fully expects that law enforcement agents would not or could not "catalogue every single movement of an individual[ ]," suggesting that to allow the government access to CSLI would contravene that decision.[90] After all, taken together, Carpenter's CSLI provided "an all-encompassing record of" his location and movement over a long period.[91] The Court seized on both the sensitive nature of the CSLI and the fact that it provided "near perfect surveillance," far removed from the abilities of a constable on foot or other eighteenth-century equivalent.[92]

After finding a search under the Fourth Amendment, the Court quickly affirmed the general presumption that warrants or warrant

---

83. Freiwald & Smith, *supra* note 66, at 219.

84. *See id.* at 219-21; *Carpenter*, 138 S. Ct. at 2213-14 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection.").

85. *See Carpenter*, 138 S. Ct. at 2231-32 (Kennedy, J., dissenting).

86. *Id.* at 2223 (majority opinion).

87. *Id.* at 2217.

88. *See id.* at 2218-19.

89. *Id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

90. *Id.* at 2217; *see also supra* notes 53-59 and accompanying text.

91. *Carpenter*, 138 S. Ct. at 2217.

92. *Id.* at 2218; *see also* Freiwald & Smith, *supra* note 66, at 221.

exceptions are required for Fourth Amendment searches.[93] Thus, a revolution in Fourth Amendment doctrine was born.[94] Or so it would seem.

Though the *Carpenter* decision may appear unprecedented at first glance,[95] it actually marks a perfectly logical and predictable development in Fourth Amendment doctrine. In fact, the Supreme Court's entire post-*Katz* nontrespassory surveillance jurisprudence, as jumbled as it may seem, could very well be reduced to a few nonconflicting principles. *Katz* introduced the principle that expectations of privacy are more important than physical spaces. *Ciraolo*, *Riley*, *Karo*, and other cases from the 1980s defined the limit of these expectations, drawing the line at potential public exposure. *Kyllo*, *Jones*, and other cases from this century have demonstrated that advancing technology does not lower the bar for public exposure. As Part II will discuss, in the correct context, a path can be traced through these cases that leads right to *Carpenter* and gives us a roadmap for the future.

II. FINDING A THROUGH LINE IN FOURTH AMENDMENT DOCTRINE

It would seem important to find a consistent direction taken by the Supreme Court on Fourth Amendment surveillance issues, especially given that major government surveillance cases since *Katz* have avoided overruling each other.[96] However, the only explicitly enumerated holding common to all these cases is the "reasonable expectation of privacy," a guideline which is, at best, "circular" and "subjective."[97]

For the purposes of this discussion, it is important to distinguish between traditional searches or seizures and government surveillance, which only became a Fourth Amendment issue after *Katz*. The dismissal of the traditional property-based approach was necessary in *Katz* to account for nontrespassory surveillance, which can

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

94. Ohm, *supra* note 65, at 358.

95. The dissenters certainly thought so. *See Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting).

96. *See supra* Part I.

97. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

be just as violative of a person's privacy as physical searches.[98] Government entry into constitutionally protected spaces or seizure of personal effects without a warrant or probable cause has always been considered violative of the Fourth Amendment.[99] The major Supreme Court cases since *Katz* listed above deal almost exclusively with nontrespassory surveillance, which should be the primary focus of any modern Fourth Amendment theory, and is therefore the focus of this Note.

A. The Many Unsatisfactory Candidates

Many potential candidates for an all-encompassing theory of Fourth Amendment rights claim to effectively unify the post-*Katz* doctrine. Some have been explicitly proposed, while others are implicit in the Court's opinions. However, most leave unsatisfactory holes in the doctrine or else fail to account for all the Court's prior decisions. Ideally, a unifying theory would include and account for every currently in-force Supreme Court decision without necessitating that any of them be overruled.

Using *Carpenter* and *Kyllo* as a lens, it might be tempting to defer to the Court's historical prerogative to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted."[100] This approach has some appeal, especially because the holding of *Kyllo* was, at least in part, motivated by the fact that when the Bill of Rights was adopted, only physical trespass would have allowed the same level of observation of activity inside the home as a thermal sensor does today.[101] Similarly, as Chief Justice Roberts pointed out in *Carpenter*, no individual investigator or team of investigators could possibly hope to gather such extensive location information as was provided by CSLI, a very recent technological development.[102] Using the "at the time the Fourth Amendment was adopted" standard would certainly go above and beyond

98. *See* Katz v. United States, 389 U.S. 347, 353 (1967).
99. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 621 (1886).
100. *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34).
101. *See Kyllo*, 533 U.S. at 34.
102. *See Carpenter*, 138 S. Ct. at 2218.

the call for protecting individuals from the threat of modern surveillance technology encroaching on private life.

But such an approach does not square with the Court's decisions in *Ciraolo* or *Florida v. Riley*—or even, quite frankly, the *Katz* test. Airplanes and helicopters were certainly not around at the time the Framers adopted the Fourth Amendment. One could easily conclude that aerial surveillance of any kind exceeds the degree of privacy that existed when the Fourth Amendment was adopted. Had Mr. Ciraolo constructed his ten-foot perimeter fence in 1791, he would have effectively ensured that the contents of his yard would remain private—and could reasonably have expected so.[103] It seems, then, that the historical standard is less of a bright-line rule and more of a general expression of society's expectations of privacy. The Court in *Carpenter* admitted as much, using "historical understandings" only to "inform[]" the analysis which has "no single rubric."[104] In essence, the historical standard is just a rewording of what "society is prepared to recognize as reasonable"[105] and therefore no less circular.

Another approach might be to refocus on the "knowingly expose[d]" language from *Katz*,[106] as the Court did in *Ciraolo* and *Florida v. Riley*.[107] The language from those opinions seems to suggest that this was indeed the direction the Rehnquist Court hoped to push Fourth Amendment jurisprudence.[108] It would be a relatively simple rule that could (at least theoretically) refine the *Katz* test without abandoning it. What has been knowingly exposed to observation from any public vantage point is necessarily not subject to a reasonable expectation of privacy. Rather than threaten the holding of *Katz*, such a rule would merely take the guesswork out of the second prong. Furthermore, it would imply that activity which has not been exposed to the public, such as activity within the walls

---

103. *See* California v. Ciraolo, 476 U.S. 207, 209 (1986).

104. *Carpenter*, 138 S. Ct. at 2213-14 (citing Carroll v. United States, 67 U.S. 132, 149 (1925)).

105. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (internal quotation marks omitted).

106. *See id.* at 351.

107. *See Ciraolo*, 476 U.S. at 213; Florida v. Riley, 488 U.S. 445, 449 (1989).

108. *See Riley*, 488 U.S. at 449 ("As a general proposition, the police may see what may be seen 'from a public vantage point where [they have] a right to be.'" (alteration in original) (quoting *Ciraolo*, 476 U.S. at 213)).

of the home or documented on a personal cell phone, would be protected by the Fourth Amendment, complying with the Court's later holdings in *Kyllo* and *Riley v. California*.

However, such a rule is plainly not conducive to the holdings in *Jones* or *Carpenter*. The legal challenges posed by location-tracking technology are relatively new, but they are no less indicative of Fourth Amendment concerns.[109] Unwarranted CSLI and GPS tracking data represent a "seismic shift[]"[110] in surveillance technology that allows the government to intrude on the "privacies of life"[111] in ways never before imagined. Surely, Mr. Carpenter's movements over those four months were exposed to the public in the sense that they took place in public spaces where he could have been observed by anyone who happened to be there.[112] Had there been a police officer present at any one of the robberies, or all four, who had seen Mr. Carpenter and positively identified him, this information would certainly not be protected by the Fourth Amendment. Rather, something about the sum total of the information makes it constitutionally protected, regardless of the fact that all of the activity in both *Jones* and *Carpenter* was technically exposed to public view.

Of course, yet another proposal is to return to a property-centric interpretation of the Fourth Amendment. This has drawn support from certain academic writers, such as Trevor Burrus and James Knight, who believe that clearer jurisprudence based on property law can help untangle the confusing legacy of the *Katz* test.[113] The idea is that the kinds of property protected by the Fourth Amendment can be expanded into areas such as CSLI without resorting to nebulous and highly subjective interpretations of reasonableness.[114] While continuing to allow the government to carry out naked-eye surveillance without trespassing, this approach can still be said to square with *Kyllo* and *Riley v. California*, because the interior of the home or personal cell phone is included in those "constitutionally protected area[s]" necessarily subject to a legitimate expectation of

109. *See Carpenter*, 138 S. Ct. at 2223.

110. *Id.* at 2219.

111. *Id.* at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

112. *See id.* ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

113. *See* Burrus & Knight, *supra* note 20, at 110-11.

114. *See id.*

privacy.[115] It would certainly fit right in with Justice Scalia's admonition that Fourth Amendment analysis does not turn on the nature of the information gathered.[116] In fact, the property-based approach could be construed to include all the Court's post-*Katz* decisions, so long as the definition of property is loose enough to include intellectual property and the like.

However, something about the property-based approach does not conform with the spirit of the Fourth Amendment, or at least not how it has been construed in the past half-century. One might very well suggest that the determinative issue in *Carpenter* was the property at stake—namely the CSLI data itself.[117] But from Mr. Carpenter's perspective, and seemingly the Court's perspective as well, that was not the case.[118] After all, Carpenter had no interest in the physical data itself; it would be hard to imagine any individual claiming actual ownership over the ones and zeros that make up CSLI. Rather, what infringed upon his expectation of privacy were the inferences drawn from the data.[119] Mr. Carpenter likely had no knowledge that this data existed before it was used to convict him, and he almost certainly would have preferred that it never existed at all. Therefore, it can hardly be said that he had a traditional property interest in the CSLI. His interest was rooted in keeping the government from inferring (via CSLI or otherwise) the details of his location over an extended period.[120] This is not property, it is information.

The crux of the issue is that CSLI falls so far outside the common understanding of "property" that it threatens to render the term meaningless. CSLI is created, managed, and controlled by cell phone service providers, not individual customers.[121] In order to fit *Carpenter* within the scope of the property-based approach, one would have to argue that individuals have a legitimate property interest in any data that describes them or their activities, regardless of

115. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

116. *See id.* at 37.

117. *See Carpenter*, 138 S. Ct. at 2211-12.

118. *See id.* at 2218-19.

119. *See id.*

120. *See id.*

121. *See id.* at 2211-12.

whether they had a hand in creating or managing it. This is, of course, an unreasonable rule. For instance, an individual cannot possibly be said to have a property interest in another's diary entry that describes her or in a newspaper article that discusses her activities. She may have a privacy interest in these sources, but it is a privacy interest that is separate and distinct from any legitimate property interest.

The oft-repeated holding in *Katz* that "the Fourth Amendment protects people, not places"[122] is indicative of the notion that the Court's post-1967 jurisprudence has really protected information and knowledge at least as much, if not more so, than property. The facts of *Katz* reflect this. It was not the location from which Mr. Katz was making a phone call that was protected by the Constitution, much less whatever physical properties a phone call can be said to exhibit.[123] What was protected was the content of the conversation, that is, information.[124]

Even in *Kyllo*, the very case in which Justice Scalia declared "quality or quantity of information" irrelevant to the Fourth Amendment analysis,[125] it was information being protected rather than property. The *Kyllo* Court's holding that activity and effects within the home are necessarily subject to Fourth Amendment protection simply generalizes a category of information that is protected.[126] Contrary to Justice Scalia's characterization of the issue, the fact that the activity in *Kyllo* took place on a traditionally protected property was only a precondition for determining the quality of the information at stake.[127] The effective outcome of *Kyllo* is that activities and effects within certain spatial contexts (namely, the home) have been determined to exhibit the quality of constitutionally protected private activity, regardless of what that activity actually is.

122. Katz v. United States, 389 U.S. 347, 351 (1967).
123. *See id.* at 354.
124. *See id.*
125. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001).
126. *See id.* at 34.
127. *See id.*

Similarly, in *Carpenter*, it was both the quantity and quality of the information at stake that led the Court to its decision.[128] This reality is not lost on academic commentators[129] and certainly was not lost on the dissenting Justices.[130] Although a property-based approach might be shaped and squeezed into the mold of post-*Katz* Fourth Amendment doctrine, it does not address the heart of the issue, and it certainly does not account for the direction that the Court seems to be headed.

B. An Effective Information-Based Approach

Given the case law discussed above,[131] the most appropriate all-encompassing Fourth Amendment theory in cases of warrantless government surveillance would take into account the private nature of certain kinds of information, without barring the government from observing or learning what any member of the public already lawfully could observe or learn (that is, what has been publicly exposed[132]). Such a theory would look something like this: absent probable cause, the government is barred from obtaining any information that could not otherwise be obtained without resorting to surveillance technology or trespassing. Such a rule is relatively simple, accounts for all post-*Katz* holdings, and provides a workable roadmap for future decisions.

*1. The Obtainable Information Approach as a Through Line for Post-*Katz *Fourth Amendment Cases*

It is easy to see how this proposed standard would encompass the holdings of *Carpenter* and *Jones*, given the "comprehensive reach" of the information at issue in those cases.[133] As pointed out by Chief

128. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (deciding based on the "depth, breadth, and comprehensive reach" of CSLI).

129. *See, e.g.*, Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 445-46.

130. *See Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting) ("[T]he Court [has] unhing[ed] Fourth Amendment doctrine from the property-based concepts that have long grounded [it].").

131. *See supra* Part I.

132. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

133. *See Carpenter*, 138 S. Ct. at 2223.

Justice Roberts, no individual person could possibly hope to compile an exhaustive account of a suspect's every movement over a period of multiple days, let alone several months.[134] Therefore, it is not the public exposure of the activity generally that matters but instead the public availability of the cumulative weight of the information, and the inferences drawn therefrom. The information at issue in *Carpenter*, as revealed by the CSLI, was only available to the government by using the CSLI technology itself, or some similar location tracking technology.[135] There is simply no way that such a vast quantity of information could be obtained otherwise. As such, it violates the rule and should be held unconstitutional. Although the *Jones* Court ultimately ruled on physical trespass grounds,[136] the same principles can apply to the location data in that case. Moreover, a five-Justice majority would have ruled in favor of Jones even if the police had not trespassed.

Riley v. California too fits nicely into the obtainable information standard. It can hardly be said that the personal information kept on a cell phone is available to anyone who does not either hack into the phone electronically or physically seize the phone itself.[137]

As discussed earlier, the *Kyllo* holding is essentially a quality-based analysis of information in certain spatial contexts.[138] In any case, a plain application of the obtainable information standard would yield the same result, and for largely the same reasons.[139] Information gathered from observing activity hidden within the walls of a private home is inaccessible, except by trespassing or using surveillance technology. That is, after all, exactly what happened in *Kyllo*.[140] Shifting the focus of the analysis from the location to the type of information at stake does not change the outcome but refines it. The information in *Kyllo*, as is the case with all information about activity and effects within the walls of a home, should

134. *Id.* at 2218.

135. *See id.*

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

137. *See generally* Riley v. California, 573 U.S. 373 (2014).

138. *See supra* notes 125-26 and accompanying text.

139. It was, in fact, the language and reasoning of the *Kyllo* holding that served as inspiration for the obtainable information standard. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

140. *See id.* at 29-30.

be protected from the government precisely because the spatial context prevents all nonsurveillance and nontrespass methods of obtaining it.

Moving further back in the Fourth Amendment timeline, *Ciraolo* and *Florida v. Riley* easily fall within the obtainable information standard as well. Those decisions hinged on the fact that a person occupying public airspace—whether or not they were trying to surveil the defendant's property—could see anything and everything the officers themselves saw.[141] Neither surveillance technology nor trespass was required to observe the marijuana growing in Mr. Ciraolo's yard or Mr. Riley's greenhouse, only an airplane or helicopter.[142] Therefore, the information at stake, namely that the defendants were growing marijuana in those locations, was obtainable without breaking the rules of the obtainable information standard. Such observation would therefore be held constitutional, consistent with the Court's opinions.

The beauty of the obtainable information standard is that it gets to the heart of the reasonable expectation of privacy test as laid out by Justice Harlan,[143] without compromising any of the values or policy concerns enumerated by the Court since *Katz*. The spirit of the two-pronged test is the preservation of private information, and the direction of the Court since adopting the test is best encapsulated by preventing the government from obtaining information otherwise unobtainable without resorting to surveillance technology or physical trespass.

2. The Information-Based Approach as a Roadmap for the Future

As technology continues to advance, the threats it poses to personal privacy will no doubt grow as well. One major problem with the property-based or public exposure standards is that they generally fail to account for the "seismic shifts" in technology that allow

141. *See* California v. Ciraolo, 476 U.S. 207, 213-14 (1986); Florida v. Riley, 488 U.S. 445, 451-52 (1989).

142. *See Ciraolo*, 476 U.S. at 213-14; *Riley*, 488 U.S. at 451-52.

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

the government to peer into formerly private areas of life.[144] The Court's Fourth Amendment theory should account for such shifts by preventing the government from using them to unduly intrude into private life. At the same time, the Court should not overly burden the government by preventing police from obtaining information that is accessible via the use of common modern technology that serves nonsurveillance purposes.

a. The Continuing Relevance of the Trespass Qualification

This Note certainly does not argue that property interests play no part in Fourth Amendment surveillance cases. Scalia's contention in *Kyllo* that the interior of a home is necessarily protected by the Fourth Amendment is not wrong, it merely misrepresents why that protection is necessary.[145] Activities and effects that are placed within the walls of a house are not magically transformed into the privacies of life merely by virtue of being there. They are protected because we expect them to be protected. There is nothing special about the interior of a house per se, except that the owner of the house exercises control over who may enter it and therefore exercises de facto control over the flow of information from within.

As such, it is appropriate to keep the "trespass" qualification from *Kyllo* attached to the obtainable information standard. In other words, if the only way information can be obtained is by trespassing on private property, then that information is protected by the Fourth Amendment. This is a sound principle, but it is incomplete. It does not account for the threat of advanced surveillance technology which does not require any such trespass.

b. Defining "Surveillance Technology"

As already noted, the obtainable information standard would effectively prevent the government from using surveillance technology to obtain information that could not otherwise have been obtained.[146] This would account for any future technological developments

144. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
145. *See supra* notes 125-26 and accompanying text.
146. *See supra* Part II.B.1.

providing access to information that was not already exposed in some way. Likewise, the enumerated concerns of the *Carpenter* Court would be readily addressed.[147] The only potential hurdle for future courts to consider would be the legal definition of "surveillance technology."

This determination could likely be made on a case-by-case basis without much trouble, but a recommended starting place should be as follows: surveillance technology is any technology used to acquire information that could not casually be acquired. As general as this may seem, it provides an important distinction, so far as the case law discussed in this Note is concerned.

Consider the airplane and helicopter at issue in *Ciraolo* and *Florida v. Riley*, respectively.[148] In each of those cases, the Court relied on the fact that any person in an aerial vehicle occupying public airspace could have observed the illegal activity, regardless of whether they were trying to surveil the property below them.[149] A passenger on a commercial flight that happened to be passing overhead could easily have "glanced down" and seen everything the police did.[150] As such, the information at stake in *Ciraolo* and *Florida v. Riley*, namely that the defendants were growing marijuana on their property, could have been casually acquired.[151] That law enforcement used this technology specifically for the purpose of surveillance is irrelevant. What matters is that the information gathered was not otherwise unobtainable.

On the other hand, technology such as the thermal sensor used in *Kyllo* would clearly fall under the definition of "surveillance technology."[152] Information about the interior of a house is unobtainable without trespassing into the home or using some kind of sense-enhancing technology.[153] Likewise, such information cannot be casually acquired in the same way as information about the contents of a fenced-in yard. Another way to think about this distinction is

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

148. *See* California v. Ciraolo, 476 U.S. 207, 209 (1986); Florida v. Riley, 488 U.S. 445, 448 (1989).

149. *See Ciraolo*, 476 U.S. at 213-14; *Riley*, 488 U.S. at 450-51.

150. *See Ciraolo*, 476 U.S. at 213-14.

151. *See id.* at 209; *Riley*, 488 U.S. at 448.

152. *See* Kyllo v. United States, 533 U.S. 27, 29-30 (2001).

153. *See id.* at 34.

to consider whether a person could acquire the information at issue without actively trying to do so. Using a thermal imaging device, or any other device capable of penetrating the walls of Kyllo's home, would necessarily require an active intent. It would be absurd to propose that any person might have "glanced" into a thermal imaging device aimed at Kyllo's house and seen everything the police had seen without meaning to see what was inside his house.

One key aspect of this definition of "surveillance technology" is that it hinges on the nature of the information, as well as the nature of the technology. Any legal definition of "surveillance technology" that rests only on the nature of the technology itself would lead to undesirable outcomes. For example, most people would likely agree that a high-resolution camera mounted on a government satellite used to monitor individuals is a "surveillance technology" by its own standards. But what if such a satellite were used to photograph a suspect who walked through a public park in the middle of the day? Regardless of the nature of the technology used to take the photographs, it would be at odds with the Supreme Court's post-*Katz* jurisprudence to say that the suspect had any legitimate privacy interest in the fact that he was in that particular public place on that particular day. Any person (or law enforcement officer) who happened to be in the park that day could have seen him without actively trying to monitor his whereabouts. In other words, the information could have been casually acquired.

In a sense, the Supreme Court has already drawn this distinction with its dual holdings in *Knotts* and *Karo*, two cases that involved the use of nearly identical electronic tracking beepers to monitor a suspect's movement.[154] Although the Court expressed its opinion in *Karo* through the language of traditional property protection, the critical difference between these two cases was that the beeper in *Knotts* was used only to track movement through public thoroughfares.[155] In *Karo*, the beeper was used to track movement within a private residence.[156] As such, the information at stake in *Knotts* could have been easily acquired by any officer who tailed the defendant on that day, whereas the information in *Karo* could only have

154. *See supra* note 43.
155. *See* United States v. Knotts, 460 U.S. 276, 281 (1983).
156. United States v. Karo, 468 U.S. 705, 714 (1984).

been acquired by trespassing had it not been for the use of the beeper technology. The *Knotts/Karo* distinction is a good example of how the exact same technology can satisfy the proposed definition of "surveillance technology" in some cases but not in others, depending on the nature of the information it has been used to acquire.

Notably, such a definition would be ambiguous when applied to simple quasi-surveillance equipment such as binoculars. A strong case could be made that activity that is observable only using binoculars or similar visual-enhancement technologies cannot be casually acquired. However, people frequently use binoculars for purposes other than surveillance. The resolution to such a case would rest on a factual determination of the likelihood that a person, using some manner of simple visual-enhancement technology for a purpose other than surveillance of the activity or property in question, could have obtained the information at issue casually, without active intent.

This ambiguity is intentional, as society's general expectation of privacy concerning such surveillance is unclear. Any definition of "surveillance technology" as the phrase is used in the obtainable information standard would need to be flexible, so as to align with the public's changing understanding of what can reasonably be expected to remain private. In any case, the legal definition proposed above would become an issue only in the narrow set of cases in which the government surveilled an individual and gathered information that could only have been acquired casually using some form of common quasi-surveillance sense-enhancing technology in a nonsurveillance manner. No such case has yet presented itself to the Supreme Court.

III. THE THORNY THIRD-PARTY DOCTRINE

After the *Katz* decision shifted the focus of Fourth Amendment inquiries away from physical property,[157] a paradox of sorts arose when it came to the legal interpretation of what one could reasonably expect to keep private. If Fourth Amendment searches were no longer tied to physical spaces the defendant occupies or owns, then

157. *See supra* notes 21-28 and accompanying text.

could a defendant claim a "reasonable expectation of privacy" regarding objects or information in the possession of another person? From a law enforcement perspective, this would be problematic: it would allow criminals to use third-party services to commit crimes without exposing themselves to the public spaces open to government surveillance.[158] The Court's solution to this conundrum was simply to make such an outlet wholly unavailable. In other words, "[u]sing a third party [will] not change the overall level of Fourth Amendment protection."[159] This standard came into being through a fusion of two cases wrestling with the application of *Katz* in the 1970s and would come to be known as the *Smith-Miller* standard.

A. The Smith-Miller *Standard*

In 1973, agents from the Alcohol, Tobacco, and Firearms Bureau (ATF) presented subpoenas to the presidents of two Georgia banks at which Mitch Miller held personal accounts.[160] The subpoenas compelled the release of all bank statements and other financial records related to Miller's accounts in their possession.[161] The banks complied with the subpoenas, and the recovered financial information revealed—as the agents had suspected—a number of financial transactions related to the illegal practice of possessing a still and distilling whiskey without paying the appropriate taxes.[162] The subpoenas had not been issued by a court, and Miller had not been informed that the subpoenas had been served.[163] His motion to suppress the evidence was denied by the district court, but his subsequent conviction was reversed by the court of appeals on Fourth Amendment grounds.[164] The Supreme Court was thus faced with the

158. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 575 (2009).
159. *Id.* at 577.
160. United States v. Miller, 425 U.S. 435, 437 (1976).
161. *Id.*
162. *See id.* at 436, 438.
163. *Id.* at 438-39.
164. *Id.*

question of whether the financial records at issue were subject to a "reasonable expectation of privacy."[165]

The Court concluded that the answer to that question must be "no."[166] The Court pointed out that Miller "can assert neither ownership nor possession" over "the business records of the banks."[167] The Court rejected Miller's contention that he justifiably relied on the continued privacy of his financial information, even after turning it over to the banks.[168] Invoking *Katz*, the Court held that Miller had "knowingly expose[d] to the public" his financial information, setting it outside the scope of Fourth Amendment protection.[169] The Court refused to accept the proposition that Miller could retain any reasonable expectation of privacy over information that he had voluntarily exposed to the public.[170]

The Court considered a similar case, *Smith v. Maryland*, in 1979, when a telephone company installed a pen register at the request of the police to record the numbers dialed from the home of a suspected criminal.[171] The register revealed that the suspect had placed a call to the phone of a robbery victim who had been receiving threatening calls from a person identifying himself as the robber.[172] Based on this evidence, the suspect was charged and convicted of robbery, over his attempted motion to suppress.[173]

Even though this case bears substantial similarities to the facts of *Katz*, the Court still found grounds for distinction. Unlike the contents of a telephone conversation, which the *Katz* Court had unequivocally placed under the protection of the Fourth Amendment, a pen register records only the number that an individual has

---

165. *See id.* at 442.

166. *Id.*

167. *Id.* at 440.

168. *Id.* at 442.

169. *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

170. *Id.* ("[C]hecks are not confidential communications but negotiable instruments to be used in commercial transactions."). Understandably, this decision ruffled the feathers of the liberals on the Court. The dissent pointed out that, although a bank's customers might voluntarily reveal their financial information to bank employees, they continue to reasonably expect the information to be kept private. *Id.* at 449 (Brennan, J., dissenting) ("A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes.").

171. 442 U.S. 735, 737 (1979).

172. *Id.*

173. *Id.* at 737-38.

dialed.[174] The Court held that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company," making it unreasonable to expect such information to be kept private.[175] The Court went on to invoke the freshly established *Miller* doctrine, comparing information shared with a phone company to financial records shared with a bank.[176] In doing so, the defendant had "assumed the risk" that the company would reveal the information to police.[177]

The holdings of these two cases have fused into what can be considered today as modern third-party doctrine. In short, any objects or information voluntarily turned over to a third party, directly or indirectly, are not subject to any expectation of privacy that society is willing to accept and are therefore not protected by the Fourth Amendment.[178] This approach has drawn its fair share of critics, almost all of whom contend that the doctrine does not accurately reflect either people's subjective expectation of privacy or society's willingness to accept it.[179]

B. Carpenter *and Third-Party Doctrine*

For many scholars, the third-party doctrine has not aged well in the era of big data. While a person's decision to turn information over to a third party may once have indicated that they lacked an expectation of privacy, modern people routinely use the internet to communicate and the cloud to store sensitive information.[180] In fact, evidence suggests that average Americans consider many types of digital information within the traditional *Smith-Miller* scope of

174. *Id.* at 741.

175. *Id.* at 742.

176. *See id.* at 744.

177. *Id.* Once again, this assertion was met by a fierce dissent objecting to the idea that a person's justifiable privacy interest is obliterated the moment they turn information over to any third party, especially in situations in which they have no choice in the matter. *Id.* at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

178. Kerr, *supra* note 158, at 563.

179. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 992-93 (2016).

180. *Id.* at 993.

third-party exceptions more private than certain other areas that are protected by the Fourth Amendment.[181]

On some level, this reflects of a problem that existed long before the advent of the cloud, a problem recognized by the dissenters in the *Smith* and *Miller* cases.[182] Namely, there is a difference between information turned over to a single source out of necessity and information voluntarily disclosed to the public at large. Fourth Amendment scholar Sherry Colb points out that "treating exposure to a limited audience as identical to exposure to the world, means failing to recognize degrees of privacy in the Fourth Amendment context."[183] These "degrees of privacy" have always existed; they have simply become more apparent as advancing technology has made it easier to access sensitive information.[184] It is not unreasonable to suggest that when people take what is private and make it public, they have forfeited their expectation of privacy.[185] But what they "seek[] to preserve as private, even in an area accessible to the public, may be constitutionally protected."[186]

The Court seemed to recognize this problem when it rendered its decision in *Carpenter*.[187] It referenced the "seismic shifts in digital technology" that have allowed detailed tracking of everyone with a smartphone, as well as the fact that such location data is not really voluntarily "shared" with the cell service companies.[188] Critically, it also called back to a notion expressed in *Riley v. California* that an individual can have a diminished privacy interest without completely abrogating all Fourth Amendment protection.[189] The Court used this reasoning (and a good bit of legal finagling) to find third-party doctrine inapplicable without overruling any part of either

181. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 184-86 (2007) (finding that most people consider a search of private emails more intrusive than pat downs or vehicle searches).

182. *See supra* notes 170, 177.

183. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

184. *See id.*

185. *Id.* at 124-26.

186. Katz v. United States, 389 U.S. 347, 351-52 (1967).

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

188. *Id.*

189. *Id.* at 2219; *see also* Riley v. California, 573 U.S. 373, 392 (2014) ("The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.").

Smith or *Miller*.[190] Of course, the only way to manage this was by focusing on the content of the information, rather than its location.[191] This would seem to suggest that some categories of information, regardless of whether they have been "voluntarily" disclosed to a third-party corporation, are simply too private to allow an unsympathetic traditional application of third-party doctrine.

C. Third-Party Doctrine and the Obtainable Information Standard

Many commentators believe that, whatever the third-party doctrine was once worth, it has lost its usefulness and should be retired in favor of a more modern understanding of privacy expectations. This may very well be true. However, it should be noted that the obtainable information standard does not require the doctrine to be overruled or even modified any more than it already has been by *Carpenter*.[192] In other words, the standard would work even if the Court chooses to retain third-party doctrine.

The third-party doctrine is based on the presumption that information willingly turned over to a third party has been "expose[d] to the public" and therefore necessarily fails the *Katz* test.[193] If need be, this presumption could carry over to an information-based approach. If information has fallen into the hands of a third party, the government need not resort to trespass or surveillance to obtain it. So long as the third party is willing to hand the information over, the third-party doctrine can be upheld with the obtainable information framework.

Taking the Court's two landmark decisions in this area as examples, it is easy to see how the obtainable information standard might apply. In the case of Mitch Miller, his bank records were voluntarily disclosed to the bank itself, at least in the sense that he

190. *See Carpenter*, 138 S. Ct. at 2220.

191. *Id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.").

192. *See id.* at 2217 (refusing to extend the *Smith-Miller* standard to cell phone location records).

193. *See* United States v. Miller, 425 U.S. 435, 442 (1976) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

knew his bank had access to the information contained within them.[194] Rather than resorting to physical intrusion or surveillance, the government simply obtained the information by taking it from the bank itself.[195] As such, there was no violation of the obtainable information standard.

The *Smith* case is more troubling, as the installation of a pen register can hardly be said not to constitute surveillance.[196] Furthermore, such a device almost certainly seems to fall within the scope of "surveillance technology" as discussed earlier in this Note.[197] However, the question is no less easily resolved. As the Court pointed out in *Smith*, unlike the content of a phone conversation, the number being dialed is willingly turned over to the phone company, as the phone call could not be carried out otherwise.[198] Therefore, although the government in this case did resort to surveillance to gather information, that information was not otherwise unavailable. The government could theoretically have casually acquired the information indirectly through the phone company, which had full access to the numbers being dialed by the defendant.[199] As such, the information at stake in *Smith* can be construed to comply with the obtainable information standard to the extent that the use of surveillance technology was not necessary.

Furthermore, this point raises a compelling distinction between the information at issue in *Smith* and in *Carpenter*. In *Smith*, the phone company's access to the numbers its clients dialed was not for the purpose of creating a log of which numbers were dialed or for identifying the people at either end of a conversation.[200] Rather, it was a collateral necessity of the company's need to connect its customers with the intended recipients of their phone calls.[201] Using this logic, it cannot be maintained that the technology allowing the company's access to the numbers Smith dialed was primarily used for the purpose of gathering the type of information at issue in that

194. *See id.*
195. *See id.* at 437-38.
196. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).
197. *See supra* Part II.B.2.b.
198. *Smith*, 442 U.S. at 742.
199. *See id.*
200. *See id.*
201. *Id.*

case. On the other hand, the CSLI data in *Carpenter*, whether accessed by the government or by the phone company, was gathered and catalogued specifically for the purpose of tracking the phone's location.[202] Therefore, the primary purpose of the computer systems that compile CSLI is, in fact, to gather the very type of information at issue in that case.[203]

In this sense, the obtainable information standard bridges the gap between traditional third-party doctrine and the holding of *Carpenter*, addressing the fears of many academic commentators on the matter.[204] Under the standard, it would not matter whether the government or a third party initially obtained the information at issue. Only the nature of the information itself and the technology used to obtain it would be relevant to the inquiry. In doing so, the obtainable information standard preserves the third-party doctrine's legitimate public interests without risking betrayal of the increasingly complex degrees of privacy afforded by modern technology.[205]

CONCLUSION

The legacy of Justice Harlan's two-prong test for identifying constitutionally protected interests is prolific and yet decidedly mixed. Traditional application of the Fourth Amendment had been relatively simple: either the government physically intruded upon a specific constitutionally protected area or there was no violation whatsoever.[206] But *Katz* opened the door for government surveillance to be judged under the framework of the Fourth Amendment, even when such surveillance did not involve physical intrusion into a protected space.[207] Such a major development prompted a slew of new questions and concerns, few of which were adequately addressed by the ambiguity and circularity of the "reasonable

202. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018); *see also* Lacambra, *supra* note 73.

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

204. *See, e.g.*, Melody J. Brannon, Carpenter v. United States*: Building a Property-Based Fourth Amendment Approach for Digital Data*, 33 CRIM. JUST. 20, 26 (2019) (stating that the third-party doctrine is "on life support" after *Carpenter*).

205. *See* Colb, *supra* note 183, at 122.

206. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (stating that the Fourth Amendment applies only to "material things").

207. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

expectation of privacy." It necessarily required the Court to broaden its focus beyond the physical realm and allow the Fourth Amendment to protect information as well as property.

The Supreme Court has avoided explicitly stating this reality for over half a century, but a cursory review of the relevant case law indicates that it has been trending in this direction. *Carpenter* was just one more nail (albeit a decisive one) in the proverbial coffin of the strictly textualist property-based approach to Fourth Amendment doctrine. Scholars may find ways to force the round pegs of *Carpenter* and *Jones* into the square holes of the property-based approach or the historical approach,[208] but these are temporary solutions which serve only to postpone the inevitable. As it turns out, modern Fourth Amendment law is tied to both the quantity and quality of the information obtained.[209]

Having recognized this, it is simple to create an all-encompassing information-based standard for cases of warrantless government surveillance that both accounts for all the Court's post-*Katz* holdings and provides a clear roadmap for the future: absent probable cause, the Fourth Amendment prevents the government from obtaining information that could not otherwise be obtained without resorting to surveillance technology or trespassing on private property.[210] Provided a proper definition for "surveillance technology" and a rough idea of how this standard would have applied to other cases, the obtainable information rule could provide some much-needed clarity for lower courts.

It may be true that the *Katz* test is somewhat "circular" and "subjective,"[211] but it has done a far better job accounting for society's evolving privacy values than a traditional application of Fourth

208. *See, e.g.*, Burrus & Knight, *supra* note 20, at 111; Brannon, *supra* note 204, at 24-26.

209. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (deciding based on the "depth, breadth, and comprehensive reach" of CSLI).

210. *See* Colb, *supra* note 183, at 125.

211. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

Amendment doctrine. Now that the digital age is well underway, it deserves to be cemented in a clean and clear rule for checking government surveillance.

Joshua L. Wagner[*]

* William & Mary Law School, J.D. candidate, 2021. I would like to thank Professors Rebecca Green and Paul Marcus for their helpful comments and suggestions, as well as their wonderful classes, which inspired this Note. I would also like to thank Jennifer Kleine for her invaluable editorial assistance and the entire staff of the *William & Mary Law Review* who worked tirelessly to make my work presentable.