Case Western Reserve Law Review

Volume 70 | Issue 2 Article 14

2019

The Erosion of *Smith v. Maryland*

Geneva Ramirez

— Comment —

THE EROSION OF *SMITH* v. *MARYLAND*

CONTENTS

INTRODUCTION

In 1979, the Supreme Court held in *Smith v. Maryland*[1] that individuals do not have a reasonable expectation of privacy in the telephone numbers they dial.[2] So the Fourth Amendment did not apply when the government requested that Smith's telephone company use a pen register to record all of the outgoing numbers dialed from his phone.[3] The Court justified its decision by emphasizing that pen reg–isters were simple mechanical devices with limited functions, recording *only* the telephone numbers dialed from the particular landline to which a register was attached.[4]

But today, pen registers are not so limited. In fact, the term no longer refers to a particular device but to *any* "device or process which records or decodes dialing . . . information,"[5] including outgoing tele–phone numbers, the date, time, and length of calls.[6] Even in 1979, it

1. 442 U.S. 735 (1979).

2. *Id.* at 745–46.

3. *Id.*

4. *Id.* at 741–43.

5. 18 U.S.C. § 3127(3) (2012).

6. *See* John T. Nockleby, *Privacy in Cyberspace: Modules I & IV*, HARV. L. SCH.: BERKMAN CTR. FOR INTERNET & SOC'Y (2002), https://cyber.harvard

was easy to infer private information from a list of telephone numbers because "phone numbers are unique to their owners."[7] Simply by using a telephone directory, phone numbers can be matched to their owners to reveal who a person was calling. The receiving party could be a friend, an addiction resource hotline, a church, or a political organ–ization. And by identifying each of these recipients, private information can be inferred about the caller.[8] These limited inferences mean that telephone numbers are not *just* telephone numbers as the *Smith* Court suggested. This is even more true today. With the development of inexpensive data storage and datamining technology, the inferences to be drawn from aggregated telephony metadata can often serve as a cost-effective proxy for the content of the conversations themselves.[9]

In *Carpenter v. United States*,[10] the Supreme Court recognized the threat to privacy posed when the government is permitted to amass and analyze large amounts of metadata about an individual.[11] It held that the Fourth Amendment applies when the government seeks to acquire at least one week's worth of an individual's cell site location information ("CSLI")[12]—location metadata automatically generated by dint of a cell phone's operation and stored by cell-service providers for business purposes.[13] The analysis in *Carpenter* marks a shift in the Court's understanding of how the Fourth Amendment applies in the context of digital metadata to protect against "too permeating police surveillance."[14]

Although aggregated telephony and location metadata can often be analyzed to yield similar (if not the same) private information, the

.edu/privacy/ [https://perma.cc/XJS3-MHYX].

7. Supplemental Declaration of Professor Edward W. Felten at 2, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-3994).

8. Declaration of Professor Edward W. Felten at 14, *ACLU*, 959 F. Supp. 2d 724 (No. 13-3994).

9. *Id.* In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court established that the contents of an individual's private conversation are subject to the Fourth Amendment's protection: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.* at 353.

10. 138 S. Ct. 2206 (2018).

11. *Id.* at 2217–18.

12. *Id.* at 2217 n.3, 2220.

13. *Id.* at 2211–12.

14. *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

Supreme Court insists that *Smith* is still good law.[15] This Comment analyzes how, despite the Court's protestations, technological developments and changes in the Supreme Court's understanding of the Fourth Amendment, as illustrated by *Carpenter*, have undermined and eroded the reasoning on which *Smith* was founded. Part I provides a detailed overview of the facts and the majority and dissenting opinions of *Smith v. Maryland*. Part II describes how the technology surrounding the acquisition and use of telephony metadata has changed in the forty years since *Smith* was decided and compares the Court's reasoning in *Carpenter* and *Smith*. Allowing the government unfettered access to telephony metadata in 1979 had drastically different privacy implications than allowing that same access today. Therefore, this Comment concludes that the same protections provided to CSLI in *Carpenter* should be extended to *Smith*'s telephony metadata.

I. *Smith v. Maryland*

A. The Facts

In 1976, as Patricia McDonough was walking home late one night, she passed a man changing a tire on his 1975 Chevrolet Monte Carlo.[16] As she neared her home, the man grabbed her from behind and forcibly took her wallet, which contained her name and address.[17] During the struggle, McDonough got a "full-face view of the robber."[18] When the man fled, she reported the incident to the police, providing a description of both her attacker and the Monte Carlo.[19]

Shortly after the robbery, McDonough began receiving "threatening and obscene" phone calls on her landline from a man identifying himself as her attacker.[20] During one such call, the caller told McDonough to step outside her house.[21] Upon doing so, she recognized the Monte Carlo she had observed at the robbery "moving slowly past her home."[22] She reported these calls to the police and, with the help of a friend, installed a recording device and recorded three or four of the calls.[23]

15. *See Carpenter*, 138 S. Ct. at 2220 (emphasizing that its decision there "do[es] not disturb the application of *Smith*").

16. Smith v. Maryland, 389 A.2d 858, 859 (Md. 1978).

17. *Id.*

18. *Id.*

19. Smith v. Maryland, 442 U.S. 735, 737 (1979).

20. *Id.*

21. *Id.*

22. *Id.*

23. *Smith*, 389 A.2d at 859.

Eleven days after the robbery, Michael Smith stopped a police officer in the general vicinity of McDonough's home and asked for help "opening the locked door of his 1975 Monte Carlo."[24] The officer who Smith stopped happened to be the same officer who had taken McDonough's statement following the robbery.[25] Recognizing the car that McDonough had described to him, the officer recorded the vehicle's license plate number.[26] When he ran the plate number, he discovered that the Monte Carlo was registered to Smith and identified Smith's telephone number.[27]

At the police's request, the telephone company installed "a pen register at its central offices to record the numbers dialed from the telephone at [Smith's] home."[28] The pen register—"a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released"[29]—recorded all of the outgoing numbers from Smith's phone but it did not record whether those calls were completed.[30] The pen register revealed that a call was placed from Smith's home phone to McDonough's residence.[31] Based on this evidence, the police secured a warrant to search Smith's home; during that search, they seized a phone book.[32] The page on which McDonough's telephone number appeared had been dog eared.[33] Smith was arrested and McDonough identified him in a lineup as the robber.[34]

Smith was indicted for robbery.[35] After his suppression motion was denied, "[t]he pen register tape . . . and the phone book" were admitted

24. *Id.*

25. *Id.*

26. *Id.*

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

28. *Id.*

29. *Id.* at 736 n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)). The Court went on to explain that "[a] pen register is 'usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line' to which it is attached." *Id.* (alterations in original) (quoting United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part)).

30. Brief of Petitioner at 5, Smith v. Maryland, 442 U.S. 735 (1979) (No. 78-5374), 1979 WL 214031, at *5.

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

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

into evidence.[36] Smith was convicted and sentenced to six years in prison.[37] The Maryland Court of Appeals affirmed, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the [F]ourth [A]mendment is implicated by the use of a pen register instal–led at the central offices of the telephone company."[38]

B. The Supreme Court's Majority Opinion

On appeal, Smith asked the Supreme Court of the United States to consider "whether the installation and use of a pen register" to reveal the outgoing telephone numbers dialed from the landline in Smith's home "constitute[d] a 'search' within the meaning of the Fourth Amendment."[39] Writing for the majority, Justice Blackmun answered with a resounding no.[40]

While acknowledging the traditional property-based conception of the Fourth Amendment,[41] Justice Blackmun explained that when "determining whether a particular form of government-initiated elec–tronic surveillance is a 'search' within the meaning of the Fourth Amendment, [the] lodestar is *Katz v. United States*."[42] In *Katz*, the Court considered whether the Fourth Amendment's warrant require–ment applied when FBI agents attached an electronic listening device to the exterior of a phone booth to record the conversations Katz carried on inside.[43] While not replacing the traditional property-based conception of the Fourth Amendment,[44] the *Katz* Court held that the Fourth Amendment applies when a government invasion "violate[s] the

36. *Id.* at 737–38.

37. *Id.* at 738.

38. Smith v. Maryland, 389 A.2d 858, 867 (Md. 1978).

39. *Smith*, 442 U.S. at 736.

40. *Id.* at 736, 745–46.

41. *Id.* at 739. Under the property-based conception of the Fourth Amendment, the Fourth Amendment applies where the government intrudes on a constitutionally protected area with the intent to find something. Weeks v. United States, 232 U.S. 383, 393–94 (1914); United States v. Jones, 565 U.S. 400, 406 n.3 (2012). In *Smith*, Justice Blackmun concluded that the property-based test did not apply to Smith's case because the information was acquired through a pen register located on the telephone company's property and thus, involved no physical intrusion into Smith's home. *Smith*, 442 U.S. at 741.

42. *Smith*, 442 U.S. at 739 (footnote omitted).

43. Katz v. United States, 389 U.S. 347, 348–50 (1967).

44. *See Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

privacy upon which [an individual] justifiably relied."[45] Justice Harlan, in his concurrence, understood the majority's language to require both that the individual "exhibited an actual (subjective) expectation of privacy" and "that the expectation be one that society is prepared to recognize as 'reasonable.'"[46] This two-prong analysis has been adopted by the Supreme Court in subsequent cases, including *Smith*.[47]

In *Smith*, though purporting to apply Justice Harlan's *Katz* analysis, the Court first asked, not whether Smith himself exhibited "an actual (subjective) expectation of privacy," but whether a reasonable person would "entertain any actual expectation of privacy in the numbers they dial."[48] This apparent misapplication of *Katz*'s subjective prong likely stems from an inherent problem with the subjective inquiry itself: the only person who has knowledge of an individual's subjective belief is that individual; for everyone else, subjective belief can only be divined through guesswork.[49] The Court attempted to circumvent this conundrum by assuming that if a reasonable person would not have believed something, odds are that the individual in question did not believe it either.[50]

In applying its modified subjective inquiry, the Court assumed that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switch–ing equipment that their calls are completed" and that "[a]ll subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[51] The Court also observed that "[m]ost phone books tell subscribers, on a page entitled 'Customer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'"[52]

---

45. *Katz*, 389 U.S. at 353.

46. *Id.* at 361 (Harlan, J., concurring).

47. *Smith*, 442 U.S. at 740–41; *see also Jones*, 565 U.S. at 406 ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*] . . . ."); Bond v. United States, 529 U.S. 334, 338 (2000); California v. Ciraolo, 476 U.S. 207, 211 (1986).

48. *Smith*, 442 U.S. at 740, 742.

49. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(c) (5th ed. 2012).

50. *See Smith*, 442 U.S. at 743.

51. *Id.* at 742. It is worth noting that the telephone in Smith's residence was listed to his father and Smith may not have been the "subscriber" to whom monthly bills were sent. *See* Brief of Petitioner, *supra* note 30, at 5.

52. *Smith*, 442 U.S. at 742–43 (quoting BALTIMORE PHONE DIRECTORY 21 (1978)).

Based on these observations and assumptions, the Court concluded that a reasonable person would know that telephone numbers must be communicated to a telephone company to complete a call and that the telephone companies have the ability—by means of pen registers or otherwise—to record those numbers.[53] As such, "[a]lthough subjective expectations cannot be scientifically gauged, it [was] too much [for the Court] to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret."[54]

Next, the Court asked, assuming Smith did have a subjective expectation of privacy, whether that expectation was "one that society [was] prepared to recognize as 'reasonable.'"[55] In concluding that any subjective expectation of privacy Smith might have was not one that society was prepared to accept, the Court relied exclusively on the third-party doctrine.[56]

The *Smith* Court explained that under the third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[57] It reasoned that by dialing McDonough's telephone number, Smith assumed the risk that the telephone company—a third-party—would make public the numbers that he dialed.[58] The Court noted that exposing information to electronic equipment, such as the telephone company's switchboard, implicated the third-party doctrine just as much as if Smith had placed his call with a human third party; that is, with the assistance of a telephone operator.[59] Furthermore, the Court held that the third-party doctrine applies equally to information communicated to a third party, whether or not that party routinely makes records preserving those communications.[60]

In sum, the Court held that Smith could satisfy neither prong of the *Katz* test. As such, the Fourth Amendment's protection did not apply and the Government was within its rights to obtain via a pen register—and without a warrant—the telephone numbers that Smith dialed from his home's landline.[61]

53. *Id.* at 743.

54. *Id.*

55. *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

56. *Id.* at 743–44.

57. *Id.*

58. *Id.* at 744.

59. *Id.* at 744–45.

60. *Id.* at 745.

61. *Id.* at 745–46.

C. The Supreme Court Dissenting Opinions

Eight Justices considered Smith's case.[62] While Justices Burger, White, Rehnquist, and Stevens joined Justice Blackmun's majority, Justice Stewart and Justice Marshall, joined by Justice Brennan, filed dissenting opinions.[63] The dissenters argued that the telephone numbers an individual dials reveal intimate information about the caller and should be subject to a reasonable expectation of privacy.[64] And both took issue with the majority's application of the third-party doctrine, though for different reasons.

1. Justice Stewart

The crux of Justice Stewart's dissent was that the majority's analysis was contrary to the holding in *Katz*. He noted that, in *Katz*, the Court observed "the vital role that the public telephone has come to play in private communication[s]"[65] and that, at the time *Smith* was decided, the private telephone had become just as vital.[66] On that basis, the *Katz* Court held that using electronic surveillance equipment to intercept the contents of an individual's telephonic communications constituted a violation of the Fourth Amendment.[67] But to complete a telephone call, not only must the caller expose to the telephone company's electronic equipment the number she dials, but she must also expose the content of her conversation.[68] To Justice Stewart, it was incongruous to hold that the caller must assume the risk that her telephone company might disclose to the government only the telephone numbers she dials and not the contents of her conversation.[69]

He rejected the majority's notion that the government's collection of dialed telephone numbers was more innocuous than its collection of the content of conversations.[70] He noted that "[m]ost private telephone subscribers may have their own numbers listed in a publicly distributed directory."[71] By cross-referencing the numbers an individual dials, the

62. Justice Powell took no part in the decision. *Id.* at 746.

63. *Id.* at 736.

64. *See id.* at 747–48 (Stewart, J., dissenting); *id.* at 748–49 (Marshall, J., dissenting).

65. *Id.* at 746 (Stewart, J., dissenting) (alteration in original) (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).

66. *Id.*

67. *See Katz*, 389 U.S. at 352–53.

68. *Smith*, 442 U.S. at 746–47 (Stewart, J., dissenting).

69. *Id.* at 746–47.

70. *Id.* at 747–48.

71. *Id.* at 748.

government "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[72]

2. Justice Marshall

Justice Marshall, like Justice Stewart, believed that telephone numbers can reveal intimate information about the person who dials them. He observed that it is not only criminals who value their privacy when making calls.[73] For example, "[m]any individuals, including members of unpopular political organizations or journalists with confid–ential sources, may legitimately wish to avoid disclosure of their personal contacts."[74] He concluded that government "access to tele–phone records on less than probable cause may . . . impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."[75]

But, unlike Justice Stewart, Justice Marshall did not focus on the conflict between the majority's reasoning and *Katz*. Instead, he attacked the assumptions upon which the majority's subjective analysis rested, identifying two fundamental flaws with the third-party doctrine.[76]

Unlike the majority, Justice Marshall did not believe that it was reasonable to expect individuals to "infer from the long-distance listings on their phone bills, and from the cryptic assurances of 'help' in tracing obscene calls included in 'most' phone books, that pen registers are regularly used for recording local calls."[77] He reasoned that, even if individuals were aware that telephone companies monitor the calls they make, "it does not follow that they expect this information to be made available to the public in general or the government in particular."[78]

Justice Marshall also believed that the third-party doctrine is "misconceived in two critical respects."[79] First, he argued that for an individual to have assumed a risk by his or her action (e.g., dialing a

72. *Id.*

73. *Id.* at 751 (Marshall, J., dissenting).

74. *Id.*

75. *Id.*

76. *Id.* at 749–51.

77. *Id.* at 748–49. Justice Marshall was clearly skeptical that most individuals (with the possible exception of Justice Blackmun) would be inclined to read their phone books thoroughly enough to be familiar with the "Consumer Information" page notifying customers that telephone companies can help track obscene calls. *See id.*

78. *Id.* at 749.

79. *Id.*

number), the individual must have a meaningful choice whether to perform that action.[80] He observed the vital role that telephones have come to play in modern society and the fact that an individual *must* convey a telephone number to his or her telephone company in order to complete a call.[81] As such, he believed that an individual's choice to convey a number to his or her telephone company was not meaningful because the only alternative was to "forgo use of what for many has become a personal or professional necessity."[82] Thus, "as a practical matter, individuals have no realistic alternative."[83]

Second, he argued that "to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections."[84] He believed that the government should not be able to dictate the scope of the Fourth Amendment's protection.[85] In his view, the third-party doctrine would allow the government to avoid the Fourth Amendment's warrant requirement "simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations."[86]

In lieu of the third-party doctrine, Justice Marshall suggested an alternative test for determining whether an individual's expectation of privacy was one that society was prepared to accept: not whether an individual assumed the risk of disclosure by communicating information to a third party, but whether an individual "should be forced to assume [a particular risk] in a free and open society."[87] To answer this question, he believed that "courts must evaluate the 'intrinsic character' of investigative practices with reference to the basic values underlying the Fourth Amendment."[88] Marshall believed that privacy is not "possessed absolutely or not at all."[89] While his proposed inquiry represented a sharp deviation from the third-party doctrine's bright-line rule, he

80. *Id.*

81. *Id.* at 749–50.

82. *Id.* at 750.

83. *Id.*

84. *Id.*

85. *Id.* at 751.

86. *Id.* at 750.

87. *Id.*

88. *Id.* at 751 (quoting Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 94 (1974) (Marshall, J., dissenting)).

89. *Id.* at 749.

argued that the vaguer standard might accommodate individuals' varying degrees of privacy.[90]

II. THE ERODING BASIS OF *SMITH*

In *Carpenter v. United States*,[91] the Supreme Court held that individuals have a reasonable expectation of privacy in the whole of their physical location as revealed by their historical CSLI—the metadata automatically generated and stored by cellular service companies every time a cell phone user makes a call.[92] *Carpenter* is the first Supreme Court case since Smith was decided in 1979 to consider how the Fourth Amendment applies to third-party-maintained meta–data.[93] The two holdings reached starkly different conclusions regarding whether these different types of metadata qualify for Fourth Amendment protection.

This Part compares the analyses in *Smith* and *Katz* to that in *Carpenter*, identifying how the Supreme Court's Fourth Amendment analysis has evolved to keep pace with the technological advancements over the last forty years (since *Smith* was decided). Though the *Carpenter* Court insisted that its decision did not overturn *Smith*, *Carpenter* suggests that while short-term use of a pen register may remain outside the scope of the Fourth Amendment, long-term surveil–lance implicates its protection.

A. The Subjective Expectation

In *Katz*, the majority held that the government's use of an electronic listening device attached to the outside of a public telephone booth "violated the privacy upon which [Katz] justifiably relied."[94] This language can be read (as Justice Harlan seemed to suggest in his concurrence[95]) to require that an individual harbor a subjective

90. *Id.* at 750–51.

91. 138 S. Ct. 2206 (2018).

92. *Id.* at 2219–20; *see also* Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, THE ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/ [https://perma.cc/YBL5-ZHHV]. CSLI is also generated when cell phones are used for other purposes, including sending a text message, using an app, or getting a push notification. *Id.*

93. *See* Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL OF RTS. J. 495, 504 (2017).

94. Katz v. United States, 389 U.S. 347, 353 (1967).

95. *Id.* at 361 (Harlan, J., concurring) ("a person [must] have exhibited an actual (subjective) expectation of privacy").

expectation of privacy to qualify for Fourth Amendment protection. But many commentators have questioned whether the majority's opinion truly requires or should require consideration of an individual's subjective expectations.[96]

Orin Kerr has argued that the subjective requirement, as originally conceived by Justice Harlan, played the role of what we think of today as an objective consideration: the third-party doctrine.[97] According to Kerr, Harlan left an interpretational clue by claiming that his two-part analysis was an "understanding of the [majority's] rule that . . . emerged from prior decisions."[98] While Harlan did not give examples of these prior cases, two lines of Fourth Amendment search cases were prevalent when *Katz* was decided: "protected-area cases, which identified the spaces that could receive Fourth Amendment protection"; and "voluntary exposure" cases, in which individuals were deemed to have relinquished Fourth Amendment protection by either exposing their protected areas to public view or inviting a government agent into those areas.[99] Against this background, Kerr posited that Harlan's objective requirement stemmed from the protected-area cases, while his subjective requirement emerged from the voluntary-exposure cases[100]:

> As originally intended, the two parts of Harlan's test each did independent work. The objective test asked whether the nature of the space invaded by the government was one that society was willing to recognize as private. On the other hand, the subjective test asked whether the individual took steps to make objectively protected spaces open to outside observation and thus yielded privacy rights against that invited observation.[101]

But in the 1970s and 1980s, a doctrinal shift occurred: the Supreme Court began analyzing issues of voluntary-exposure from an objective standpoint and replaced the original subjective standard with a "purely subjective standard."[102] That reinterpretation, however, has rendered

96. LAFAVE, *supra* note 49.

97. Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113, 115 (2015).

98. *Id.* at 124 (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

99. *Id.* at 124–26.

100. *Id.* at 126.

101. *Id.*

102. *Id.* at 114, 128–30. Although some courts still "requir[e] a person to 'exhibit' or 'manifest' an expectation of privacy," that requirement is now duplicative of the third-party doctrine. *See id.* at 130–31.

the subjective requirement virtually functionless.[103] While a minority of courts applying the subjective standard retain Justice Harlan's original formulation—requiring that "a person . . . 'exhibit' or 'manifest' an expectation of privacy"[104]—this analysis has now been made redundant by the third-party doctrine.[105]

The subjective requirement also lacks any outcome-determinative effect when applied as a "purely subjective standard."[106] The Supreme Court has acknowledged that, if the Fourth Amendment protected only individuals who subjectively expected privacy, then the government could thwart the Fourth Amendment's warrant requirement by simply conditioning individuals to never expect privacy.[107] For example, by announcing that the National Security Agency is secretly collecting cellphone metadata about citizens, the government's collection of those records would fall outside of the Fourth Amendment's scope because individuals could no longer retain a subjective expectation of privacy. Even in those cases where government action has not altered the scope of an individual's subjective expectations, the court is faced with the further problem of attempting to divine purely subjective expectations, which inherently can only be truly known by the individual in question.[108]

The *Smith* Court, interpreting the subjective element as a purely subjective standard, attempted to determine Smith's subjective expect–ation of privacy by assessing whether a reasonable person generally "entertain[s] any actual expectation of privacy in the numbers [she] dial[s]."[109] Ultimately, it determined that people—and Smith by proxy—generally do not subjectively entertain such an expectation.[110] But this determination was not outcome-determinative because the Court also found that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private,

103. *Id.* at 131–33; Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979); Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1984) (emphasizing the importance of the objective element over the subjective).

104. Kerr, *supra* note 97, at 130.

105. *Id.* at 130–31.

106. *See id.* at 131.

107. *See id.* at 132–33; *see also Smith*, 442 U.S. at 740 n.5; *Hudson*, 468 U.S. at 525 n.7.

108. *See, e.g.*, *Smith*, 442 U.S. at 743 (assessing what a reasonable person might have thought were Smith's subjective expectations and admitting that "subjective expectations cannot be scientifically gauged").

109. *Id.* at 742. The Court seemingly ignored the possibility that Smith was not a reasonable person.

110. *Id.*

this expectation is not 'one that society is prepared to recognize as "reasonable."'"[111]

Due to these deficiencies, the subjective requirement has largely become a "phantom doctrine."[112] An empirical study of all 2012 Westlaw-reported cases that purported to use the *Katz* test revealed that fifty-seven percent of those cases did not mention the subjective test.[113] Of those that did, only twelve percent actually applied the test, and in no case was the subjective test outcome determinative.[114]

This phasing-out of the subjective requirement is reflected in recent Supreme Court cases.[115] For example, in *Carpenter*, the Court quoted *Smith*'s understanding of the *Katz* test, explaining that a governmental intrusion qualifies as a Fourth Amendment search when "an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable.'"[116] But despite reciting the traditional standard, the Court engaged in no subjective analysis.[117] These cases suggest that the Supreme Court, while frequently reciting Harlan's two-step formulation of the *Katz* test, has abandoned the subjective requirement. As such, a person's subjective expectations are not relevant to the contemporary understanding of the Fourth Amendment's protections.[118]

111. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

112. Kerr, *supra* note 97, at 114–15.

113. *Id.* at 114.

114. *Id.*

115. *See* Kyllo v. United States, 533 U.S. 27, 32–35 (2001) (reciting the two prongs of the reasonable-expectation-of-privacy test, but applying only the objective prong); United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring); *id.* at 422–23 (Alito, J., concurring); Riley v. California, 573 U.S. 373, 381 (2014) (declaring simply that "the ultimate touchstone of the Fourth Amendment is 'reasonableness'" and not mentioning the subjective requirement).

116. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting *Smith*, 442 U.S. at 740).

117. *Id.* at 2213–14.

118. Even if the *Smith* Court's understanding of the subjective element is still valid, the factual bases for the Court's decision—(1) monthly phone bills contain a list of long-distance numbers dialed; and (2) phone books contain a "customer information" page notifying customers that telephone companies can help identify troublesome callers—are no longer true. *See Smith*, 442 U.S. at 742–43.

Today, more than half of U.S. homes do not have landlines. Tracey Lien, *More Than Half of U.S. Households Have Ditched Landline Phones*, L.A. TIMES (June 6, 2018), https://www.latimes.com/business/technology/la-fi-tn-landline-cellphone-20180606-story.html [https://perma.cc/9DPD-L6Y4]. More than 53.9% of households now rely exclusively on cell-phone

B. The Objective Expectation

1. The Nature of the Challenged Activity

In *Smith*, the Court held that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'"[119] In coming to this conclusion, the Court explained that the *Katz* analysis must "begin by specifying precisely the nature of the state activity that is challenged."[120] In *Smith*, that activity was the installation and use of a pen register.[121] Early pen registers were mechanical devices that could be attached to a particular telephone line in a telephone company's central offices.[122] Whenever dial pulses passed through the line, the pen register would automatically record the dialed numbers as dashes on paper tape.[123] The functions of the pen register in *Smith*—based on the Court's opinion—seem to have been quite limited, recording *only* the telephone numbers dialed without revealing any other identifying information.[124] The Court found this functional limitation significant:

---

service, and that number is climbing. *Id.* And most cell-phone bills do not contain a list of numbers the user has dialed over the preceding month. *See*, *e.g.*, *Current Customers: Learn About Your Monthly Bill*, SPRINT https://www.sprint.com/en/support/solutions/account-and-billing/tutorial-monthly-bill.html [https://perma.cc/Z7EK-JMWD]; *Introducing Your New AT&T Bill*, AT&T, https://www.att.com/ecms/dam/att/consumer/help/pdf/Wireless-Sample-Bill-Guide.pdf [https://perma.cc/U8U4-L2FX]. This shift means that most Americans no longer receive a monthly reminder that their cell-phone-service providers are recording their telephony metadata. Furthermore, the accessibility of information online has rendered phone books a relic of the past. In 2019, the iconic Yellow Pages stopped printing. The company hoped that the final editions, printed in 2018, would become "souvenirs." Patrick Greenfield, *Yellow Pages to Stop Printing from January 2019*, THE GUARDIAN (Sept. 1, 2017), https://www.theguardian.com/media/2017/sep/01/yellow-pages-to-stop-printing-from-january-2019 [https://perma.cc/H676-KVHC].

Because a reasonable person in today's society would not have access to the same information that an individual might have possessed in 1979, it is questionable whether the Court's subjective analysis in *Smith* remains applicable.

119. *Smith*, 442 U.S. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

120. *Id.* at 741.

121. *Id.*

122. William A. Claerhout, *The Pen Register*, 20 DRAKE L. REV. 108, 109 (1970).

123. *Id.* at 110.

124. *Smith*, 442 U.S. at 741.

> [A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. . . . "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[125]

Today's pen registers, however, are not so limited. The term no longer describes a mechanical device attached to a land line. Instead, *pen register* has come to mean any device or process that records information similar to that recordable by traditional pen registers.[126] In addition to the telephone numbers called from a particular phone, contemporary pen registers also record the date, time, and length of calls.[127] This information is already gathered by telephone companies for their own business purposes, making its production relatively easy.[128]

The development of ancillary technologies like inexpensive data storage[129] and data mining[130] also challenges the *Smith* Court's assertion that the content of communications is deserving of Fourth Amendment protection while metadata is not. The Court recognized those developments in *Carpenter*. There, the state activity at issue was the government's warrantless acquisition of Carpenter's historical CSLI, data "that provide[d] a comprehensive chronicle of [his] past move–ments."[131] Like telephone numbers, CSLI is composed of metadata. As such, CSLI is not just a collection of points plotted onto a map, but it includes, among other things, the identification number associated with the radio antenna the phone connected to ("Cell ID"), the date and time the connection was made, and *the telephone number or numbers*

125. *Id.* (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

126. *See* 18 U.S.C. § 3127(3) (2012) (defining *pen register* as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication").

127. *See* Nockleby, *supra* note 6.

128. *See id.*

129. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 151–53 (2014).

130. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435–36 (2008).

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

involved.[132] By analyzing this metadata, an individual's location can be inferred.[133]

But the *Carpenter* Court did not hold that Carpenter had a reasonable expectation of privacy in his discrete CSLI records. Rather, it held that he had a reasonable expectation of privacy in his CSLI records aggregated over the course of seven days or more.[134] This focus on aggregated metadata versus discrete data points is a response to the aggregation problem: the fact that when metadata is amassed in sufficient quantities it can be analyzed by computer programs to reveal "useful correlations within data sets not capable of analysis by ordinary human assessment."[135]

The information that can be gleaned from these correlations can act as a proxy for content.[136] From the patterns and sequences in which "calls occur, when they occur, how often they occur, and between which numbers,"[137] an individual's habits can be revealed and his social network mapped:

> Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations.[138]

Some analysts have discovered correlations between callers' relative power and social statuses based on the time it takes for the parties to call each other back and at what times they call.[139]

Obtaining information through metadata analysis is often far easier and less expensive than it would be to obtain the same information by way of content *because* metadata is structured by nature,[140] allowing it

132. Matthew Tart et al., *Historic Cell Site Analysis—Overview of Principles and Survey Methodologies*, 8 DIGITAL INVESTIGATION 185, 185 (2012).

133. *Id.*

134. *Carpenter*, 138 S. Ct. at 2217 n.3.

135. Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 42 (2014); *see also* Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579 (2017); Declaration of Professor Edward W. Felten, *supra* note 8, at 8.

136. Declaration of Professor Edward W. Felten, *supra* note 8, at 14.

137. *Id.* at 9–10 (quoting PEN-LINK LTD., UNIQUE FEATURES OF PEN-LINK V8, at 5 (2008)).

138. *Id.* at 16.

139. *See id.* at 17.

140. *See id.* at 7–8.

to be inexpensively stored and efficiently analyzed.[141] By contrast, human speech is relatively unstructured and its analysis must take into account factors including language, dialect, social customs, and speech impediments.[142] These factors make it functionally impossible for analysts to analyze content on a large scale.[143]

So why was the *Smith* Court not concerned about the aggregation problem? Most likely because computer analysis of huge datasets was not possible before digital storage became economical.[144] In 1972, half a megabyte of memory—500,000 bytes—could cost as much as $100,000 or $613,775.12 today when adjusted for inflation.[145] This means that one byte of memory—which can store about one character, e.g., 'A,' '$,' or '1'[146]—would have cost $1.22 in today's dollars.[147] So, in 1972, the amount of memory needed to store a ten-digit phone number would have cost about $2.00 (about $12.00 today). By comparison, one terabyte—one trillion bytes—of memory can be purchased on Amazon for $19.99[148]—enough memory to store 100 billion ten-digit telephone numbers.[149]

Though both *Carpenter* and *Smith* considered the government's acquisition of telephony metadata, the Courts reached the opposite conclusion on whether the Fourth Amendment applies.[150] The *Smith*

141. *Id.* at 8.

142. *See id.*

143. *See id.* at 7–8, 11.

144. *Id.* at 8.

145. *See* Three-Seventy Leasing Corp. v. Ampex Corp., 528 F.2d 993, 995, 996 n.2 (5th Cir. 1976); U.S. INFLATION CALCULATOR, https://www.usinflationcalculator.com [https://perma.cc/MNE3-3ST5] (last updated Dec. 11, 2019).

146. *CS101 Introduction to Computing Principles: Bits and Bytes*, STAN. U., https://web.stanford.edu/class/cs101/bits-bytes.html [https://perma.cc/4TDE-DFDY] (last visited Oct. 2, 2019).

147. *See* U.S. INFLATION CALCULATOR, *supra* note 145.

148. *1 TB USB Flash Drive Memory Stick for Laptop/PC/Computer*, AMAZON, https://www.amazon.com/Flash-Memory-Rotatable-Laptop-Computer/dp/B07NY9WR28/ref=sr_1_4?keywords=terabyte+flash+drive&qid=1570049813&sr=8-4 [https://perma.cc/A4W6-V7H2] (last visited Dec. 31, 2019).

149. *See* Declaration of Professor Edward W. Felten, *supra* note 8, at 5–6 (calculating that it would take approximately fifty terabytes annually to store all U.S.-generated call records).

150. *Compare* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("[W]hen the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."), *with* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) ("[Smith] in all probability entertained no actual expectation of

Court viewed telephone numbers in isolation;[151] the *Carpenter* Court focused not only on the numbers that constitute CSLI, but also on what those numbers mean in the context of technological innovations.[152] The *Carpenter* Court noted that intimate information that one might expect to keep private can be *inferred* from CSLI analysis, including a person's "familial, political, professional, religious, and sexual associations."[153] These same privacies can be inferred from the aggregated telephony metadata gathered by a pen register.[154] And the *Carpenter* Court believed that the threat to privacy posed by CSLI datamining was exacerbated by the fact that the use of this technology is both practical and economical.[155] Again, datamining telephony bears the same hall–marks.

The way *Carpenter* described the nature of CSLI shows that the Court's view of metadata has changed in two significant ways. First, metadata should not be viewed in isolation, but in the context of other technological innovations that analysts use to infer the private details of an individual's life. For example, rather than looking only at the information collected and the direct means of its collection (e.g., telephone numbers collected by a pen register), the Court must widen its focus to consider ancillary technologies, such as the government's ability to manipulate that metadata after its acquisition by using

---

privacy in the phone numbers he dialed, and . . . if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

151. *Smith*, 442 U.S. at 744.

152. *Carpenter*, 138 S. Ct. at 2211–12, 2216–17.

153. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). By rejecting the government's contention that CSLI did not infringe on Carpenter's reasonable expectation of privacy because that data did "not on their own suffice to place [Carpenter] at the crime scene," the Court reminded us that, in *Kyllo*, it had rejected the proposition that "inference insulates a search." *Id.* at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 37 n.4 (2001)). Stated differently, information from which intimate inferences can be drawn is not immune to the Fourth Amendment's warrant requirement solely because the information itself reveals no intimate information if that inference is never drawn.

154. *See* Declaration of Professor Edward W. Felten, *supra* note 8, at 14, 20. The logic underlying the inference is simply different. Just as "individuals often go to particular locations for particular purposes," Brief of Technology Experts as Amici Curiae in Support of Petitioner at 29, Carpenter v. United States, 138 S. Ct. 2206 (No. 16-402) (emphasis omitted), "certain telephone numbers are used for a single purpose," Declaration of Professor Edward W. Felten, *supra* note 8, at 14.

155. *Carpenter*, 138 S. Ct. at 2217–18; *see also* Brief of Technology Experts, *supra* note 154, at 28–29.

datamining programs. Second, even if privacy concerns are not implicated by the government's acquisition of discrete pieces of metadata, they may be implicated by that data's aggregation over time.[156] Viewed through these lenses, allowing the government to collect telephone numbers without judicial oversight has very different privacy implications today than it did in 1979.

It is unlikely, in light of *Carpenter*, that the Court would find an expectation of privacy in discrete telephone numbers dialed from a particular phone. But the threat to privacy posed by the aggregation problem regarding both CSLI and telephony metadata indicates that the Fourth Amendment should impose a limit on the long-term use of pen registers to collect telephony metadata.

2. The Third-Party Doctrine

The *Smith* Court held that, despite the intimate nature of the information the government acquires, that information is not protected by the Fourth Amendment if the third-party doctrine is implicated.[157] The Court reasoned that by typing numbers into his telephone, Smith voluntarily conveyed the information to his telephone company, and, in doing so, he assumed the risk that the telephone company would reveal those numbers to the government.[158] This clear cut analysis seems to suggest that the Court understood the third-party doctrine to be a bright-line rule: If an individual conveys information to a third party, then that individual has assumed the risk that the third party will disclose the information.[159]

But in the wake of *Carpenter*, the third-party doctrine's scope has become uncertain. In holding that the third-party doctrine does not apply to CSLI, the Court seems to have created a new test for determining the doctrine's application.[160] This new test requires courts to consider: (1) whether the information at issue was voluntarily exposed; and (2) whether the information was sensitive.[161]

156. Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 437 (noting that the *Carpenter* Court held that "while *each* public movement may be exposed and hence unprotected by *Katz*, the *aggregate* of such movements may qualify for Fourth Amendment protection"); *see also Carpenter*, 138 S. Ct. at 2217 ("individuals have a reasonable expectation of privacy in the whole of their physical movements").

157. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

158. *Id.* at 744.

159. *Id.* at 743–44.

160. *Carpenter*, 138 S. Ct. at 2219–20.

161. *See id.*

The Court gave two reasons for its conclusion that CSLI "is not truly 'shared.'"[162] First, it noted that "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."[163] Though the Court did not cite Justice Marshall's dissent in *Smith*, its reasoning is identical: if there is no reasonable alternative, there is no voluntary choice for the purposes of the third-party doctrine.[164] But the *Carpenter* Court gave no explanation for distinguishing between telephone numbers collected by contemporary "pen registers" and CSLI, which is partially composed of telephone numbers collected by telephone companies for their business records.[165]

The second reason the *Carpenter* Court gave for why CSLI is involuntarily shared is that CSLI is generated "by dint of [a cell phone's] operation, without any affirmative act on the part of the user beyond powering up."[166] The only way to avoid generating CSLI is to avoid using a cellphone all together.[167] But just as "you can[not] effectively self-regulate to control when or whether you share your location, without turning your phone off,"[168] you cannot prevent your telephony metadata from being recorded without ceasing to use your phone for its primary purpose: to call people. It is true that typing a specific telephone number into a phone is more voluntary than a cell phone generating a CSLI record when it automatically fetches emails. The purpose it serves, however, is to allow the Court to avoid overturning its precedents rather than to either "secure 'the privacies

162. *Id.* at 2220.

163. *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

164. *See supra* Part I.C.2; *see also Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.") (citation omitted).

165. Caminker, *supra* note 156, at 446 ("[T]he dissents in *Miller* and *Smith* were equally reasonable in claiming that people must use banks and landlines. The Court in *Carpenter* offered no reason to distinguish among these arguable imperatives of daily life, nor thoughts on the comparative societal necessity of using credit cards, computers, cars, or cardiologists.") (footnote omitted).

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

167. *Id.*

168. Caminker, *supra* note 156, at 446.

of life' against 'arbitrary power'"[169] or "place obstacles in the way of a too permeating police surveillance."[170]

In addition to the voluntariness of the exposure, the *Carpenter* Court considered the nature of the information sought.[171] It reasoned that "*Smith* . . . did not rely solely on the act of sharing. Instead, [it] considered 'the nature of the particular [information] sought' to deter–mine whether 'there is a legitimate "expectation of privacy" concerning [its] contents.'"[172] As at least one commentator has noted, this assertion is a forced reading of *Smith* and its predecessors.[173] Nevertheless, the Court seems to have "injected data sensitivity into the third-party equation."[174]

The Court concluded that CSLI is not subject to the third-party doctrine because it "is an entirely different species of business record";[175] that is, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* . . . and the exhaustive chronicle of location information casually collected by wireless carriers today."[176] But due to the close similarities between the CSLI at issue in *Carpenter* and the telephone metadata at issue in *Smith*, this line-drawing is dubious.[177] The Court insisted that pen registers have limited capacity and that "telephone call logs reveal little in the way of 'identifying information.'"[178] The fundamental problem with the Court's analysis is that it compared the privacy implications of allowing the government to collect telephony metadata in the context of 1979's datamining technology and CSLI in the context of 2018's datamining technology. Had the Court considered telephony metadata in a modern context, its analysis may well have produced a different outcome.

CONCLUSION

In *Katz*, the Court concluded that the trespass doctrine was "no longer . . . controlling" because it had been "so eroded" by the Court's

169. *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

170. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

171. *Id.* at 2219.

172. *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

173. *See* Caminker, *supra* note 156, at 448.

174. *Id.*

175. *Carpenter*, 138 S. Ct. at 2222.

176. *Id.* at 2219.

177. *See supra* Part II.B.1.

178. *Carpenter*, 138 S. Ct. at 2219 (quoting Riley v. California, 573 U.S. 373, 400 (2014)).

evolving Fourth Amendment jurisprudence.[179] Today, over fifty years after *Katz*, the Court, despite its insistence to the contrary, finds itself in a similar position. The government's technological capabilities and the Court's evolving jurisprudence have eroded the basis on which the majority in *Smith v. Maryland* concluded that dialed telephone numbers are not entitled to Fourth Amendment protection. Recognizing the "seismic shifts in digital technology" that allowed the government to track Carpenter's location[180]—metadata aggregation and analysis—the Court made significant modifications to then-existing Fourth Amend–ment doctrine. These modifications should apply to telephony metadata acquired by the long-term use of modern "pen registers," bringing them under the protection of the Fourth Amendment's warrant requirement.

Geneva Ramirez†

179. Katz v. United States, 389 U.S. 347, 353 (1967).

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

† J.D. Candidate, 2020, Case Western Reserve University School of Law. The author would like to thank Professor Michael Benza for his feedback and encouragement throughout the writing of this Comment. Additional thanks to everyone on the Case Western Reserve Law Review for their many hours of editing and review.