DEFYING EXPECTATIONS: A CASE FOR ABANDONING *KATZ* BY ADOPTING A DIGITAL TRESPASS DOCTRINE

Joshua Schow*

I. INTRODUCTION

The rapid advances of twenty-first century technology have afforded the American government enormous intrusive latitude. America might be far from hanging placards emblazoned with the proclamation that "Big Brother Is Watching You,"[1] but concerns about the domineering encroachment of sprawling government surveillance are well founded.[2] More localized methods of conducting criminal investigations also deserve similar apprehensive scrutiny.[3]

The Fourth Amendment protects the rights of American citizens to secure their persons, houses, papers, and effects against unreasonable search and seizure.[4] Modern Supreme Court jurisprudence, however, has inadvertently undermined these protections as the challenges of modern technology rapidly outpace the Court's ability to anticipate the unique difficulties presented by sophisticated surveillance. The genesis

 J.D., Stetson University College of Law, 2020. B.A, cum laude, Patrick Henry College, 2014.

1. GEORGE ORWELL, 1984 at 2 (New Am. Library, 1950).

2. Types of government surveillance that have raised concerns have ranged from publicly-announced government policies to clandestine operations meant to escape public notice. Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 979–82 (2008) (describing Bush-era mass surveillance programs such as the Terrorist Surveillance Program); David D. Cole, *After Snowden: Regulating Technology-Aided Surveillance in the Digital Age*, 44 CAP. U. L. REV. 677, 686–89 (2016) (describing the massive NSA surveillance programs, which persisted in the Obama-era).

3. For example, Rushin has explored how the "increasingly digitally efficient investigative state" has come "dangerously close to [becoming a] 'wholesale surveillance'" operation. Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 282–83.

4. U.S. CONST. amend IV.

of this problem began with the Warren Court's decision in *Katz v. United States*.[5]

According to the doctrine developed in *Katz*, the "touchstone" of the Fourth Amendment is whether an individual has a reasonable expectation of privacy in the actions they are undertaking.[6] As Justice Harlan wrote in his concurrence to *Katz*, such expectations are determined by evaluating whether a person manifests a subjective expectation of privacy and whether "society is prepared to recognize" that expectation as reasonable.[7] Justice Harlan's two-part test is now the centerpiece of the Supreme Court's Fourth Amendment jurisprudence.[8] Even though *Katz* has been law for more than fifty years, the Court has struggled to create a consistent, understandable methodology for applying the test.[9] The Supreme Court's continued reliance on the *Katz* doctrine's "reasonable expectations of privacy" test will continue to create significant legal challenges because the *Katz* doctrine is too amorphous to provide much value in the modern age of technology.[10]

This Article argues that the Supreme Court should abandon the *Katz* doctrine and return to the property interests embedded in the original meaning of the Fourth Amendment. The Supreme Court could better protect citizens by evaluating government actions in terms of trespass. Rather than focus exclusively on physical trespass, the Court should expand the trespass paradigm to digital trespass. As the Fourth Amendment prohibits the government from physically trespassing into constitutionally protected areas,[11] so too must the Fourth Amendment protect individuals from digital trespass. By extending the property paradigm to cover information in the digital world, the Court can more easily address new technological challenges as they arise without resorting to speculations about what society might believe about ethereal notions of privacy.

---

5. 389 U.S. 347 (1967).

6. *See* Oliver v. United States, 466 U.S. 170, 177 (1984) (referring to the reasonable expectation of privacy as "the touchstone of [Fourth] Amendment analysis").

7. Katz v. United States, 389 U.S. 347, 361 (1967).

8. Smith v. Maryland, 442 U.S. 735, 740–41 (1979) (stating that "this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action").

9. *See* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) (laying out the difficulties that have persisted with the *Katz* doctrine).

10. *See infra* pt. III (discussing the criticisms and defenses of the *Katz* doctrine).

11. Florida v. Jardines, 569 U.S. 1, 5 (2013).

Part II of this Article examines the *Katz* doctrine's history by first exploring the origins of the Fourth Amendment and then considering how the Supreme Court's understanding of the Amendment evolved. Part III lays out some of the most salient criticisms and defenses of the *Katz* doctrine. Part IV evaluates two recent proposals for re-imagining the Fourth Amendment. Part V synthesizes previous case law and existing commentary to propose an alternative digital trespass doctrine. Part V also explores how the digital trespass doctrine would function, how it solves the issues *Katz* created, and what potential challenges this new doctrine could present.

II. HISTORY OF THE KATZ *DOCTRINE*

Fourth Amendment jurisprudence traces back to the early 1760s to English concerns with general warrants.[12] While the founding American generation expressed similar concerns about general warrants, they focused less on the technical violations that occurred and more on the normative rights violated by the English practice. The Supreme Court initially understood the Fourth Amendment in terms of property. *Katz*, however, radically shifted the Fourth Amendment toward privacy. Beginning in 2001, the Supreme Court briefly entertained a modified property-centric Fourth Amendment paradigm, but recent decisions illustrate that the Court has returned to the *Katz* doctrine's exclusive privacy focus.

A. Original Concerns Informing the Fourth Amendment

General warrants originally evolved from constabulary habits of obtaining warrants to search any location the constables suspected could harbor stolen goods.[13] The general warrant then gradually expanded to other applications, such as searching any location for politically seditious papers or effects.[14] In 1761, Bostonian customs officials used a writ of assistance to search untaxed goods that an

12. Broadly, English commentators have expressed alarm over the British Crown's use of broad search warrants to conduct a search without much restrictions. Legal scholars of the time began denouncing these practices as an abuse of the sanctity of the home. *See, e.g.*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1235–40 (2016).

13. John M.A. DiPippa, *Is the Fourth Amendment Obsolete?—Restating the Fourth Amendment in Functional Terms*, 22 GONZ. L. REV. 483, 504 (1987–1988).

14. *Id.*

American colonist, James Otis, was attempting to import.[15] Despite Otis' protest, the colonial court held that the writ was legal.[16]

Four years later, the English considered whether general search warrants violated the rights of citizens.[17] In the case of *Entick v. Carrington*,[18] the Queen's Bench evaluated the actions of the local constables who were authorized under the authority of a general warrant to search Entick's personal papers for seditious content.[19] The Bench condemned the use of general warrants, saying it infringed on the "sacred" rights of the people to secure their property from trespass.[20] Shortly after the *Entick* decision, the English Parliament expressly outlawed general search warrants.[21]

Despite the express prohibition of general warrants in the English mainland, the British Parliament passed the Townshend Act in 1767 which, among other measures, reauthorized the use of general writs to perform customs searches in the American colonies.[22] Many colonists were outraged over this perceived overreach.[23] In response, numerous states adopted language in their Declarations of Rights that explicitly condemned the use of general warrants.[24] The early colonial experience with searches and seizures, however, was not restricted to concerns about general warrants.[25] Rather, the colonists objected because searches and seizures "unduly interfered with private life."[26] Thus, while the general warrant incited practical concerns, the founding generation was also troubled by how these actions impinged on the general rights

15. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV 547, 561 (1999).

16. *Id.*

17. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772 (1994).

18. Entick v. Carrington (1765) 95 Eng. Rep. 807 (K.B.), http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html.

19. *Id.*

20. *Id.* (noting that "our law holds the property of every man so sacred" that any trespass, even ones that result in no damage to property, are expressly prohibited).

21. Parliament abolished the general search warrant in 1766, but the general arrest warrant was not outlawed. DiPippa, *supra* note 13, at 506.

22. Davies, *supra* note 15, at 566.

23. DiPippa, *supra* note 13, at 508–10; Davies, *supra* note 15, at 674–88.

24. VA. CONST. OF 1776, art. X; PA. CONST. OF 1776, art. X; *see also* DiPippa, *supra* note 13, at 508–10; Davies, *supra* note 15, at 674–88 (both explaining the general evolution of colonial constitutional rights related to search and seizure clauses in state constitutions).

25. While Davies claims that the founding generation narrowly focused on general warrants, Davies, *supra* note 15, at 590, Donohue provides a more complete picture of the concerns animating the founding generation, Donohue, *supra* note 12, at 1240–44.

26. Donohue, *supra* note 12, at 1240.

of the people.[27] With these broader concerns in mind, Madison drafted, and the first Congress passed, the Fourth Amendment using expansive language which prohibited all "unreasonable searches and seizures."[28]

B. The Property Era for the Fourth Amendment

The Supreme Court first dealt with the expansion of law enforcement authority almost one hundred years after the drafting of the Constitution in *Boyd v. United States*.[29] Customs officers seized thirty-five cases of plate glass claiming they were fraudulently shipped.[30] The authorities attempted to prove the fraud by seizing invoices from Boyd, but Boyd objected claiming protection against self-incrimination.[31] The Court said the *Entick* decision invoked the "very essence of constitutional liberty and security" because it laid out why it was necessary to protect the "sanctity of a man's home and the privacies of life."[32] The Court ruled the search and seizure of Boyd's property was repugnant to the Constitution because it was an "invasion of his indefeasible right of personal security, personal liberty, and private property."[33]

While *Boyd* largely adhered to the broader understanding of the Fourth Amendment as protecting tangible things from overbroad search and seizure,[34] *Olmstead v. United States*[35] began an era of narrowly focusing on physical trespass.[36] In 1928, the Supreme Court considered whether the warrantless interception of telephone messages violated the Fourth Amendment.[37] Writing for the majority, Justice Taft understood the Fourth Amendment as a provision, which protected material things from unreasonable government intrusion because such

27. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 765–66 (2009) ("The framers of the [A]mendment were less concerned with a right against general warrants than with the broader rights those warrants infringed.").

28. U.S CONST. amend. IV; *see also* Donohue, *supra* note 12, at 1298–1305 (noting the history of the Amendment's drafting and passage).

29. Boyd v. United States, 116 U.S. 616 (1886).

30. *Id.* at 618.

31. *Id.* at 618–19.

32. *Id.* at 630.

33. *Id.*

34. Davies, *supra* note 15, at 728–29.

35. Olmstead v. United States, 277 U.S. 438 (1928).

36. William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 17 (2001); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004) [hereinafter Kerr, *Technologies*].

37. *Olmstead*, 277 U.S. at 457.

actions constitute a trespass on property.[38] Since there was no physical trespass in the wiretap, the Court held that such interception of phone conversations did not violate the Fourth Amendment.[39] The *Olmstead* Court noted, however, that Congress could still protect phone messages by passing legislation to render the intercepted conversations inadmissible in criminal trials.[40]

Although Congress moved to afford some protections to phone conversations,[41] the *Olmstead* trespassory analysis remained intact for nearly forty years until the Warren Court.[42] The Warren Court, however, did not immediately dispense with *Olmstead*'s trespassory analysis. *Silverman v. United States*[43] was the Warren Court's first opportunity to consider wiretapping. In *Silverman*, law enforcement recorded conversations in the home by using a microphone with a spike that physically attached to the outside of the house's wall to record conversations.[44] Based on these facts, the Court declined to review the cases that followed *Olmstead*, but instead found law enforcement violated the Fourth Amendment because of the "unauthorized physical penetration into the premises occupied by the petitioners."[45] Initially, it seemed the Warren Court was reluctant to challenge *Olmstead*. Slowly, however, the Warren Court began eroding the core rationale of *Olmstead* by increasingly focusing on privacy considerations.

C. From Property to Privacy—Protecting "People, Not Places"[46]

1. Katz *Background*

Understanding *Katz* first requires some analysis of the Warren Court's posture toward the *Olmstead* decision. Legally and scholastically,

38. *Id.* at 464.

39. The Court noted that the language of the Amendment cannot be "employed beyond the possible practical meaning of houses, persons, papers, and effects." *Id.* at 465.

40. *Id.*

41. Nardone v. United States, 302 U.S. 379, 381–82 (1937) (holding the Federal Communications Act of 1934 limited the use of wiretapping).

42. *See* Goldman v. United States, 316 U.S. 129, 136 (1942) (declining to overrule *Olmstead*); On Lee v. United States, 343 U.S. 747, 753 (1952) (rejecting multiple justifications for departing from *Olmstead*'s holding).

43. 365 U.S. 505 (1961).

44. *Id.* at 506–07.

45. *Id.* at 509.

46. Katz v. United States, 389 U.S. 347, 351 (1967).

Olmstead endured significant controversy.[47] Supreme Court Justices and academics alike heavily criticized *Olmstead*'s framework for analyzing the Fourth Amendment. In 1942, Justice Murphy criticized *Olmstead* for its "narrow, literal construction" of the Fourth Amendment's principles.[48] Justice Brennan believed *Olmstead* was premised on a "misreading of the history and purpose of the Amendment."[49] Even in *Silverman v. United States*,[50] Justice Douglas wrote a concurrence lamenting the rule established by *Olmstead*, saying it ensured Fourth Amendment cases would turn on "the trivialities of the local law of trespass" and "the kind of electronic equipment employed."[51] Some scholars commented that the *Olmstead* regime yielded a "stilted and anachronistic"[52] legal paradigm that failed to adequately "regulate the use of new technologies."[53]

Even before the Warren Court decided *Katz* in 1967, the Court developed a firm conviction that privacy was a key constitutional right, both as a general constitutional principle and as a specific right embedded in the Fourth Amendment. Six years prior to the *Katz* decision, the Warren Court described the Fourth Amendment as protecting "the right to privacy."[54] In *Griswold v. Connecticut*,[55] widely considered a groundbreaking Warren-era case,[56] the Court characterized the Fourth Amendment as one of the key "zones of privacy" "emanat[ing]" from the "penumbras" of the Bill of Rights.[57] In the same year *Katz* was decided, the Warren Court had already

47. *See* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 2–6 & n.6 (2009) (explaining that the negative public reactions to the *Olmstead* decision included passage of the Federal Communications Act in 1934, a presidential pardon for Olmstead from Franklin D. Roosevelt, and a vigorous legal debate about the decision specifically and the acceptability of wiretapping more generally).

48. Goldman v. United States, 316 U.S. 129, 140 (1942) (Murphy, J., dissenting).

49. Lopez v. United States, 373 U.S. 427, 459 (1963) (Brennan, J., dissenting).

50. Silverman v. United States, 365 U.S. 505 (1961).

51. *Id.* at 513 (Douglas, J., concurring).

52. Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1088 (1987) (exploring some of the scholarly criticism of the *Olmstead* decision).

53. Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 247 (1993) [hereinafter Cloud, *Pragmatism*].

54. Mapp v. Ohio, 367 U.S. 643, 650–51 (1961).

55. Griswold v. Connecticut, 381 U.S. 479 (1965).

56. *See, e.g.*, Lackland H. Bloom, Jr., *The Legacy of* Griswold, 16 OHIO N.U. L. REV. 511, 511 (1989) (calling *Griswold* a landmark decision recognizing the existence of the constitutional right to privacy); David Helscher, Griswold v. Connecticut *and the Unenumerated Right of Privacy*, 15 N. ILL. U. L. REV. 33, 33–34 (1994) (discussing the legacy and impact of *Griswold*).

57. *Griswold*, 381 U.S. at 484.

invalidated a New York statute permitting wiretapping because the "statute's blanket grant of permission to eavesdrop" was overbroad and failed to "safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[58] Additionally, in a case involving a search under exigent circumstances, the Warren Court specifically noted that the "principal object of the Fourth Amendment" was "privacy rather than property."[59] When viewed with the proclamations of earlier cases in mind, it is difficult to maintain the common scholarly characterization that *Katz* revolutionized Fourth Amendment jurisprudence.[60] Rather, *Katz* can be more effectively understood as an articulation of the principles the Warren Court, except for Justice Black,[61] had already carefully articulated in prior decisions.[62]

Some might object to characterizing *Katz* as unremarkable for the Warren Court by pointing out that *Silverman* might be read as an endorsement of the *Olmstead* regime.[63] The Warren Court's subsequent decisions, however, suggest their refusal to extend the precedent "by even a fraction of an inch"[64] was animated less by a faithful preference for *Olmstead* and more by an active, yet cautious, opposition to it.

58. Berger v. New York, 388 U.S. 41, 60 (1967); *id.* at 53 (quoting Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 528 (1967)).

59. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 304 (1967).

60. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974) (saying the *Katz* decision "marks a watershed in [F]ourth [A]mendment jurisprudence"); Tracey Maclin, Katz*,* Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 56 (2002) (proclaiming that "the holding and logic of *Katz* was revolutionary"); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 650 (1985) (characterizing *Katz* as a "monumental theoretical achievement" that liberated the Fourth Amendment by considering the "values underlying" the Amendment); Wilkins, *supra* note 52, at 1087 (explaining that "*Katz* revolutionized [F]ourth [A]mendment search analysis"); Quin M. Sorenson, Comment, *Losing a Plain View of* Katz*: The Loss of A Reasonable Expectation of Privacy Under the Readily Available Standard*, 107 DICK. L. REV. 179, 183 (2002) (arguing that "[t]he Supreme Court continued to follow the *Olmstead* approach until the seminal decision in *Katz v. United States*").

61. Katz v. United States*,* 389 U.S. 347, 364 (1967) (Black, J., dissenting) (stating, as the sole dissenting member of the Court, "I do not believe that the words of the Amendment will bear the meaning given them by today's decision"). Justice Black also dissented in *Griswold v. Connecticut*, 381 U.S. 479, 507 (1965) (Black, J., dissenting) and in *Berger v. New York*, 388 U.S. 41, 70 (1967) (Black, J., dissenting).

62. This is not to suggest that *Katz* was not a significant decision. This Author merely seeks to illustrate that characterizing *Katz* as an abrupt break from prior precedent would be anachronistically simplistic. The more precise characterization would be that the Warren Court revolutionized Fourth Amendment jurisprudence and *Katz* was the denouement of that revolution.

63. The Court unanimously decided the case without undermining the *Olmstead* trespassory property paradigm. Silverman v. United States, 365 U.S. 505, 506 (1961).

64. *Id.* at 512.

Although the Warren Court disliked the property paradigm, the facts in *Silverman* did not lend themselves to properly dismantling the *Olmstead* framework. But *Katz* provided a perfect factual scenario where no physical trespass occurred.[65] Prior to *Katz*, the Warren Court carefully set the stage to articulate their full reasoning for conceptualizing the Fourth Amendment as protecting privacy, not just property.

2. Katz *Reasoning*

While the Warren Court might have previously only provided a general explanation of how it understood the Fourth Amendment, *Katz* formally shifted from the trespass- and property-based regimen to one which focused on privacy concerns.[66] In *Katz*, the Court considered whether using an electronic listening and recording device to record a conversation that occurred in a public telephone booth constituted a "search" under the Fourth Amendment.[67] Answering the question in the affirmative, the Court completed its reimagining of the Fourth Amendment by declaring it "protects people, not places."[68] The majority held that whatever any citizen "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[69]

While the majority opinion in *Katz* was heavy on proclamations, it did not clearly lay out how future courts should apply these new principles.[70] Justice Harlan, however, supplied the necessary analytical framework. In his concurring opinion, he interpreted the majority's

65. *See Katz*, 389 U.S. at 352.

66. Kevin Emas & Tamara Pallas, United States v. Jones*: Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 118 (2012) (explaining how *Katz* disrupted the trespass paradigm of *Olmstead*).

67. *Katz*, 389 U.S. at 348. For a more complete history and background on how the Court formulated the *Katz* decision, see Harvey A. Schneider, Katz v. United States*: The Untold Story*, 40 MCGEORGE L. REV. 13 (2009).

68. *Katz*, 389 U.S. at 351. This proclamation seems quite puzzling because the plain text of the Fourth Amendment firmly contradicts this assertion. The Warren Court is correct that the Amendment does not protect places exclusively, but it most certainly *does* protect places (the home); it also protects things which are not people (papers and effects). U.S. CONST. amend. IV.

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

70. Perplexingly, the Warren Court did not explicitly overrule *Olmstead*; something Justice Black pointed out in his dissent. *Id.* at 372 (Black, J., dissenting). The majority instead implied *Olmstead* was *already* no longer good law because the "underpinnings" of the decision "have been so eroded . . . that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Id.* at 353. Subsequent decisions, however, seemed to accept that *Katz* overruled *Olmstead*. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 280 (1983). That is, until the Court noted that "[t]he *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test." United States v. Jones, 565 U.S. 400, 409 (2012). *See infra* pt. II.E.

doctrine to mean that a person is afforded constitutional protections when they manifest a subjective expectation of privacy and "society is prepared to recognize" that expectation as reasonable.[71] The Supreme Court later adopted Justice Harlan's two-part test as the standard paradigm for assessing Fourth Amendment claims.[72]

D. Restrictions and Exceptions to the *Katz* Doctrine

While the Warren Court ostensibly intended the *Katz* doctrine to allow future courts the latitude to afford greater protections to individual privacy, the development of the third-party doctrine in the Burger Court quickly restricted the reach of *Katz* protections. In *United States v. Miller*,[73] the Court considered whether bank records seized under subpoena power were protected by the Fourth Amendment.[74] The Court reasoned that the Fourth Amendment does not protect information disclosed to third-parties because the individual willingly disclosed the information fully understanding the third-party might share that information with others.[75] Concluding that *Katz* contemplated the consequences of knowingly exposing information to the public, the Court decided that Miller had no reasonable expectation of privacy.[76]

Shortly afterwards, the Burger Court demonstrated that *Miller* was not a fluke. In *Smith v. Maryland*,[77] the Court considered whether phone numbers recorded by a pen register installed upon law enforcement's request absent a warrant should be considered a search under the Fourth Amendment.[78] The Court decided that information exposed to a third party in the ordinary course of business has "no legitimate expectation of privacy."[79] The Court reasoned that the phone number Smith dialed had to be conveyed to the telephone company, and therefore "his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."[80] In this regard, both

71. *Katz*, 389 U.S. at 361.
72. California v. Ciraolo, 476 U.S. 207, 211 (1986); United States v. Knotts, 460 U.S. 276, 280–81 (1983); Smith v. Maryland, 442 U.S. 735, 740 (1979).
73. 425 U.S. 435 (1976).
74. *Id.* at 438–39.
75. *Id.* at 443.
76. *Id.* at 442–43.
77. 442 U.S. 735 (1979).
78. *Id.* at 737–38.
79. *Id.* at 744.
80. *Id.* at 743.

Miller and *Smith* significantly restrict how *Katz* is applied. Indeed, scholars have heavily criticized the third-party doctrine for these restrictions of Fourth Amendment protections.[81]

E. The Property Era (Briefly) Reconsidered

For the next twenty-two years after the *Smith* decision, the Court closely followed the *Katz* doctrine when considering Fourth Amendment search and seizure cases.[82] Beginning in 2001, however, the Court began analyzing the Fourth Amendment in terms of trespass again. In *Kyllo v. United States*,[83] the Court evaluated whether the use of a thermal imaging device to detect the presence of marijuana plants in a house constituted a "search" within the meaning of the Fourth Amendment.[84] Justice Scalia, writing for the Court, noted that *Katz* has been criticized as "circular, and hence subjective and unpredictable."[85] Rather than attempt to conduct a full *Katz* analysis, the Court found that "there is a ready criterion [for establishing a reasonable expectation of privacy], with roots deep in the common law"—the protection of privacy within one's own house.[86] The Court held that any activity that reveals details of the home—no matter how insignificant—that would be otherwise unknown without a physical intrusion into the house, constitutes a

81. 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, 122–23 (2002) (explaining how Fourth Amendment jurisprudence has conflated the risk of exposing information with consent to expose information to third parties); DiPippa, *supra* note 13, at 490 (saying the Court's decision in *Smith* "does violence to the plain meaning of the [F]ourth [A]mendment and its intent"). Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1045 (2018-2019) (arguing the third-party doctrine ignores the sensitivity of information, making disclosure an absolute bar to privacy expectations); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 13 (2012) [hereinafter Slobogin, Jones] (demonstrating how immunizing government acquisition of information gathered from third parties defeats the key protections of privacy embedded in the Fourth Amendment).

82. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83 (1998) (expectation of privacy as a "guest" in an apartment); California v. Greenwood, 486 U.S. 35 (1988) (expectation of privacy regarding garbage they dispose); Dow Chemical v. United States, 476 U.S. 227 (1986) (expectation of privacy regarding aerial photography); United States v. Karo, 468 U.S. 705 (1984) (expectation of privacy related to a tracker installed in a container); United States v. Knotts, 460 U.S. 276 (1982) (expectation of privacy related to a tracker installed in a container).

83. 533 U.S. 27 (2001).

84. *Id.* at 40.

85. *Id.* at 34.

86. *Id.*

search and is presumptively unreasonable without the authorization of a warrant.[87]

Justice Scalia expanded upon this trespass theory in *United States v. Jones*.[88] In *Jones*, the Court considered whether the installation of a GPS device on Jones' car and subsequent monitoring of his movements constituted a search.[89] Justice Scalia, again writing for the majority, explained that *Katz*, rather than supplanting the enumerated property interests in the Fourth Amendment, merely added to the Court's traditional trespass analysis.[90] As such, the Court found law enforcement actions constituted a search because they "physically occupied private property for the purpose of obtaining information."[91] While the holding in *Jones* was unanimous, Justices Sotomayor and Alito were critical of Justice Scalia's approach to the *Katz* doctrine.[92]

In *Florida v. Jardines*,[93] the Court again examined Fourth Amendment protections on trespass grounds. The Court considered whether law enforcement officers' use of a drug sniffing dog on the front porch of a home was a search in violation of the Fourth Amendment.[94] Justice Scalia, writing again for the majority, examined the case according to the "Fourth Amendment's property-rights baseline."[95] The Court held law enforcement violated the Fourth Amendment's protections because they trespassed into a constitutionally protected area with the purpose of obtaining information.[96] While the majority specifically declined to analyze the case under the *Katz* paradigm,[97]

87. *Id.* at 40.

88. 565 U.S. 400 (2012).

89. *Id.* at 402–03 (holding there was a search because attaching a GPS device to a car amounted to a physical trespass on private property).

90. *Id.* at 409. Subsequent cases reaffirmed Justice Scalia's analysis. Byrd v. United States, 138 S. Ct. 1518, 1526 (2018) (noting that *Katz* "supplements, rather than displaces" traditional property-focused analysis of the Fourth Amendment); Florida v. Jardines, 569 U.S. 1, 11 (2013) (finding *Katz* adds to, rather than subtracts from, "the traditional property-based understanding of the Fourth Amendment").

91. *Jones*, 565 U.S. at 404.

92. *Id.* at 414 (Sotomayor, J., concurring) (expressing reservation about the majority's trespassory analysis because "physical intrusion is now unnecessary to many forms of surveillance"); *id.* at 418–19 (Alito, J., with Ginsburg, Breyer, Kagan, JJ., concurring) (saying the majority's reasoning is "unwise" because it "strains the language of the Fourth Amendment," is unsupported by "current Fourth Amendment case law," and creates a "highly artificial" framework).

93. 569 U.S. 1 (2013).

94. *Id.* at 3.

95. *Id.* at 11.

96. *Id.* at 5.

97. *Id.* at 11 (stating that "we need not decide whether the officers' investigation of Jardines' home violated his expectation of privacy under *Katz*").

Justice Kagan's concurrence did.[98] Unlike Justices Alito and Sotomayor in *Jones*, however, Justice Kagan was less skeptical of the property-based approach, noting that "[i]t is not surprising that . . . property concepts and privacy concepts should so align."[99] The Court's focus on Fourth Amendment trespass, however, did not last long.

F. Return to the *Katz* Doctrine

Kyllo and *Jones* represent a resurgence of property-focused Fourth Amendment analysis. This renaissance, however, was short-lived. With the death of Justice Scalia, the Court returned to evaluating Fourth Amendment claims exclusively under the *Katz* doctrine.[100] In *Carpenter v. United States*,[101] the Court considered whether the use of cell-site location information (CSLI) to track an individual's location constituted a search. The majority held that, because the data revealed such extensive information about the defendant, the government "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[102] The Court, while not directly overruling the third-party doctrine, decided not to apply *Smith* and *Miller* because they determined the depth and breadth of the data collected placed CSLI data in a whole different category than telephone numbers and bank information.[103]

Carpenter presented the Court with an opportunity to reconcile questions about the usefulness of the third-party doctrine[104] with the

98. *Id.* at 12–13 (Kagan, J., concurring).

99. *Id.* at 13.

100. *Carpenter v. United States*, however, was not the first time the Court confronted digital searches. In *Riley v. California*, the Court considered whether law enforcement officials needed a warrant to search digital data on the cell phone of an individual who has been arrested. 573 U.S. 373, 378 (2014). The Court determined that "[m]odern cell phones, as a category, implicate privacy concerns far beyond" what has been contemplated by the search incident to arrest exception to the warrant requirement. *Id.* at 393. Because of these privacy concerns, the Court decided law enforcement could not apply the search incident to arrest exception to data stored on a cell phone. *Id.* at 403.

101. 138 S. Ct. 2206 (2018).

102. *Id.* at 2119.

103. *See id.* at 2217 (holding that the Court cannot "extend *Smith* and *Miller* to cover these novel circumstances").

104. In the context of modern communication technology, academics have recognized a strict application of the third-party doctrine would render all data disseminated to cell phone and internet providers searchable without virtually (pun intended) any need for a warrant. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403 (2004); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by*

advent of modern technology and the latent problems with the *Katz* doctrine.[105] The Court's holding, however, confuses both issues. Justice Kennedy argued in his dissent that *Smith* and *Miller* should apply to CSLI data because the majority's reasoning "unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases."[106] Alternatively, Justices Thomas and Gorsuch agreed with the majority—that the third-party doctrine should not be used for tracking cell phone data cases—but argued the majority's rationale failed to reconcile the third-party doctrine with *Katz*.[107]

While the *Carpenter* decision certainly moves Fourth Amendment jurisprudence away from a *carte blanche* application of the third-party doctrine, the decision provides little in the way of guidance needed to "draw . . . nuanced categorical distinctions" between when the third-party doctrine applies and when it does not.[108] This failure to provide guidance has begun to play out in the lower courts, which have repeatedly interpreted *Carpenter* narrowly by declining to extend the rationale of the decision to non-CSLI technology.[109] Similarly, while the Court favorably cited *Kyllo*[110] and *Jones*,[111] the majority abandoned Justice Scalia's property-based trespass analysis. But the Court did little to articulate a standard that clarified the latent problems associated with *Katz*.

III. ANALYZING THE LEGACY OF THE KATZ *DOCTRINE*

Scholarly examination of the *Katz* doctrine has exposed several logical and analytical problems with the framework the Warren Court created. These critics have focused predominantly on the difficulties of logically applying the doctrine as well as the seeming futility of attempting to apply the doctrine in a modern context where technology

Society," 42 DUKE L.J. 727, 732 (1993) [hereinafter Slobogin & Schumacher, *Empirical Look*]; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002).

105. *See infra* pt. III.

106. *Carpenter*, 138 S. Ct. at 2224 (2018) (Kennedy, J., dissenting).

107. *Id.* at 2236 (Thomas, J., dissenting).

108. Gentithes, *supra* note 81, at 3–4.

109. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. FORUM 943, 960 (2019) (analyzing 200 federal and state opinions citing *Carpenter* in early 2019).

110. *See Carpenter*, 138 S. Ct. at 2214, 2218.

111. *See id.* at 2213, 2214 n.1.

has quickly outpaced judicial considerations for privacy protections. Nevertheless, the *Katz* doctrine is not without its defenders. There are, after all, reasons the Supreme Court has upheld the doctrine for more than fifty years. This Part explores these criticisms and defenses of the *Katz* doctrine.

A. Criticism of *Katz*

1. The Impracticality of Judges Acting as Social Proxies

If the proclamation that the Fourth Amendment protects "what society is prepared to recognize as reasonable"[112] is taken seriously, judges cannot apply the *Katz* doctrine without referencing broader social beliefs. Empirical data gathered from surveys are the most easily accessible method for assessing public beliefs.[113] Despite the Court's insistence on considering societal expectations of privacy, judges are not well situated to evaluate these expectations.[114] Judges attempting to understand how the American public defines their privacy expectations will encounter a variety of methodological complications.[115] Often, legal practitioners do not have the proper training or expertise in statistical analysis to understand—let alone accurately navigate—these complications, particularly when evaluating emerging technology.[116] Despite these difficulties, some commentators believe courts can sift through multifarious data with little trouble.[117] The labyrinth of case law that has developed around expectations of privacy suggests this optimism is misplaced.

While Justice Harlan in *Katz* said privacy was dependent on what society was prepared to recognize, neither he nor the majority reference

112. Katz v. United States, 389 U.S. 347, 361 (1967).

113. *See* Slobogin & Schumacher, *Empirical Look*, *supra* note 104, at 732. While some courts rely on legislation to inform their rulings, such an approach is severely limited by signal noise and federalism complications. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1140–49 (2017) [hereinafter Kerr, *Legislation*] (explaining the significant limitations to looking to legislation as a means of defining society's expectations).

114. *See generally* Maclin, *supra* note 60, at 74–75 (discussing the difficulties judges have in evaluating privacy concerns because of the considerable technological shifts of the twenty-first century).

115. *See* Amitai Etzioni, *Eight Nails into* Katz*'s Coffin*, 65 CASE W. RES. L. REV. 413, 415–16 (2014).

116. Kerr, *Technologies*, *supra* note 36, at 858 (arguing that the courts "lack the institutional capacity to easily grasp the privacy implications of new technology they encounter").

117. Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV 1588, 1600 n.58 (2010) [hereinafter Slobogin, *Reply*].

any empirical literature on societal expectations of privacy.[118] Indeed, most subsequent opinions applying the *Katz* doctrine contain only the barest analysis of what society is prepared to recognize, with nary a reference to empirical literature on whether society actually attaches any privacy expectations to the activities contemplated in the case.[119] The question of whether the judiciary *can* properly interpret empirical data, therefore, might be entirely ancillary to Fourth Amendment jurisprudence. The Supreme Court simply *does not* use empirical data to determine whether society is prepared to recognize an expectation as reasonable. Perhaps the Court does consider empirical literature when crafting their opinions, but the Court has habitually failed to cite or even obliquely reference such information. Alternatively, the Court might simply believe the task of reviewing empirical literature is best left to the lower courts. Both alternatives seem dubious. More plausibly, the Justices are substituting their own reasoning and assumptions for the will of the people. The doctrine creates a paradox where a neutral observer—the judge—is expected to guess what society expects. The real question embedded in the *Katz* doctrine, therefore, is not whether society is prepared to recognize an expectation of privacy as reasonable,

118. The majority merely asserted "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures." Katz v. United States, 389 U.S. 347, 359 (1967). Likewise, Justice Harlan simply says an expectation of privacy in a phone booth is reasonable because it "is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.* at 361 (Harlan, J., concurring).

119. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (asserting that allowing law enforcement access to seven days of cell-site records violated societal expectations of privacy while providing no empirical support for the proposition); Florida. v. Jardines, 569 U.S. 1, 24 (2013) (arguing through analogy and hypotheticals that "[i]t is clear that the occupant of a house has no reasonable expectation of privacy with respect to odors that can be smelled by human beings who are standing in such places"); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (suggesting with no empirical support that "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period"); California v. Ciraolo, 476 U.S. 207, 212–13 (1986) (choosing instead to formulate the test as societal values protected by the Fourth Amendment, the Court declared—without further explanation—the curtilage is a protected space "both physically and psychologically, where privacy expectations are most heightened"); United States v. Knotts, 460 U.S. 276, 281 (1983) (arguing from precedent rather than empirical information that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"); Smith v. Maryland, 442 U.S. 735, 742 (1979) (supporting their contention that "people in general [likely do not] entertain any actual expectation of privacy in the numbers they dial" with citations to several other cases and law review articles which generally discussed current uses of pen registers); United States v. Miller, 425 U.S. 435, 442 (1976) (determining that the Court "perceive[d] no legitimate 'expectation of privacy' in the[] contents" of bank records without considering any external evidence for that perception other than to reference congressional passage of the Bank Secrecy Act).

but whether the judiciary is willing to acknowledge that society recognizes such expectations. This analytical approach runs contrary to the language the Court has repeatedly relied on to justify their analysis[120] and creates an entirely arbitrary system of constitutional protections, which rise and fall on the whims of judicial preference.

2. The Illusory Pursuit of Society's Expectations

Even if the Supreme Court took the task of assessing societal expectations seriously, empirical data might be too limited to generate legally reliable results. Psychometricians and statisticians have long warned of the analytical and procedural difficulty of providing representative, statistically valid, and accurate population-level survey data.[121] While courts certainly should not disqualify all sociological data, the limitations of survey research illustrate why it is so difficult to rely on public opinion to fashion constitutional protections. For example, scholars have empirically evaluated American expectations of privacy and found that they do not always align with the Supreme Court's understanding of those expectations.[122] Thus, the Supreme Court's own jurisprudence on expectations of privacy has not followed what society actually believes.

Other researchers question whether courts can even formulate reliable understandings of societal expectations of privacy.[123] After reviewing empirical research on whether lay individuals considered searches intrusive, they noted that expectations of privacy are often highly dependent on context typically ignored by judicial considerations.[124] Some empirical research also indicates that social

120. As the Supreme Court acknowledged in *Rakas v. Illinois*, expectations of privacy must be based on "reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." 439 U.S. 128, n.12 (1978).

121. In survey science, sound survey results must be both internally and externally validated. Slobogin & Schumacher, *Empirical Look*, *supra* note 104, at 744. Internal validity considers the consistency of an individual test taker's results and external validity evaluates whether the results are repeatable over different test groups. *Id.* Developing internal and external validity survey instruments presents a formidable challenge to survey specialists because one survey often cannot reliably capture accurate cross-sections of a broad population. Oscar H. Gandy Jr., *Public Opinion Surveys and the Formation of Privacy Policy*, 59 J. SOC. ISSUES 283, 284 (2003).

122. *See* Slobogin & Schumacher, *Empirical Look*, *supra* note 104, at 740–42.

123. *See* Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy*," 11 U. PA. J. CONST. L. 331, 352 (2009).

124. *Id.* (finding that courts should consider that their empirical results indicate opinion "changes depending on certain facts of the case, characteristics of the actors in a case, or characteristics of reviewers of the case"). Other commentators have noted the notion of privacy is

expectations of privacy are conditioned, based on the seriousness of the alleged crime necessitating the search.[125]

Furthermore, the expectations of privacy are not unidirectionally set by individual citizens, but often are subject to complex institutional pressures such as proclamations of the President, laws passed by Congress, cases decided by the courts, and even the policies of major corporations.[126] Allowing these institutional pressures to determine what expectations of privacy are reasonable would undermine the fundamental policy justification for elevating privacy to a constitutionally protected right.[127] A court applying the *Katz* doctrine is therefore placed in the untenable situation of sifting through conflicting data, tenuous notions of reliability, and multi-directional signals from authoritative institutions. Such complications make it extraordinarily difficult, if not impossible, to render sound judgment on what society recognizes as reasonable.

3. The Subjectivity of Malleable Perceptions

Assuming, for the sake of argument, that the courts can arrive at a defensible understanding of societal expectations of privacy to render decisions on the case before them, a court must then confront the reality that social expectations change, often quite rapidly, with the advent of new technology.[128] Whether initiated by government officials or major corporations, actors have institutional incentives to find new and creative ways to collect, monitor, and analyze data generated by

---

relative compared to law enforcement interests in prosecuting crimes, thereby restricting the normative values of the Fourth Amendment. DiPippa, *supra* note 13, at 497.

125. *See* Blumenthal et al., *supra* note 123, at 352–53; Slobogin & Schumacher, *Empirical Look*, *supra* note 104, at 762–64.

126. Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 844 (2002); *see also* Etzioni, *supra* note 115, at 416 (cataloging various scenarios where large institutional actors can easily alter social expectations of privacy through policy declarations).

127. Kerr, *Technologies*, *supra* note 36, at 871 (finding that institutional limitations on the courts prevent judicial rules from developing flexibility, which can accommodate technological changes while still protecting the Fourth Amendment).

128. Casey, *supra* note 2, at 1027 (finding expectations of privacy are necessarily based on "fluctuating normative standard[s]"); DiPippa, *supra* note 13, at 484 (explaining that technological advances are rapidly outpacing constitutional protections); James D. Phillips & Katherine E. Kohm, *Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right of Privacy*, 18 RICH. J.L. & TECH. 1, 2–3 (2011) (describing how the mass collection of sensitive personal information and increasing prevalence of surveillance technology have generated significant public concern from lawmakers and citizens).

citizens.[129] Recent revelations of the repeated privacy violations of major social media platforms have only accelerated growing public cynicism regarding privacy in the digital realm.[130] Even if courts could arrive at reliable conclusions about societal expectations of privacy, the conclusions a court reaches in one case could rapidly shift with the introduction of new technology. That court would then have to develop the societal awareness to acknowledge dramatic shifts in public opinion, overturn its previous precedent, and institute a new rule to keep up with ever evolving societal expectations.[131] Courts are institutionally ill-equipped to adjudicate such rapid social changes.

The *Katz* doctrine presents an even greater conceptual problem with technology because the doctrine treats expectations of privacy as a binary test—there either are reasonable expectations of privacy or not.[132] This artificial binary ignores the analytical complexity of social expectations. As other scholars have noted, society recognizes that there are "degrees of privacy" afforded to information, particularly when it comes to information technology.[133] Collapsing expectations of privacy into a binary existence or non-existence only undermines the fundamental interests *Katz* intended to protect.[134] The simplistic binary becomes apparent when examining cases where the Court has readily abandoned or analyzed its way out of consistently applying the *Katz* doctrine.[135] The lack of clarity in the Court's recent *Carpenter* decision

129. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (exploring issues with public online records, consumer profiling tools, and Radio Frequency Identification (RFID) Tags).

130. *See* Abigail W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH CENTER (June 4, 2018), http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (noting that half of Americans surveyed thought they had either not much control or no control at all over the amount of electronic information that is collected about them).

131. Even Justice Alito—usually a staunch defender of the *Katz* doctrine—acknowledged that "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., with Ginsburg, Breyer, and Kagan, J.J., concurring).

132. *Katz* finds that information "may be constitutionally protected" when any man "seeks to preserve [it] as private, even in an area accessible to the public." Katz v. United States, 389 U.S. 347, 351 (1967). If the information is constitutionally protected, then a search has occurred. However, if there is no constitutionally protected information based on the privacy expectations, then no search is said to have occurred.

133. Colb, *supra* note 81, at 123.

134. *Id.*

135. Florida v. Riley, 488 U.S. 445, 451–52 (1989) (determining that observations of a semi-closed greenhouse from a helicopter circling a house four hundred feet in the air was not an unreasonable search); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that a law

has made this problem particularly acute. While there may be some special categories that deserve special attention, the Court did not extrapolate on how one ought to determine whether these categories exist or what degree of protection they should be afforded.[136]

Determining whether the constitutional rights of citizens are diminished or enhanced by societal expectations undermines the normative rights embedded in the Constitution. The American liberal democratic system presupposes certain rights are protected as givens, subject to change only when immense public and political pressure will deem it necessary to change those rights.[137] Grounding the Fourth Amendment in terms of society's expectations, however, subjects constitutional rights to the very whims of "an interested and overbearing majority"[138] that the Founders hoped to avoid. Suppose public opinion changed significantly in the next two decades so that a substantial majority of Americans had no expectation of privacy in their digital communication, fully expecting the government to not only track and surveil their activities, but also digitally capture and review the content of their private conversations. Following the *Katz* doctrine would require the Court to find that society is not prepared to recognize any expectations that one's conversations would be free from government surveillance. Therefore, no unreasonable search occurs when the government sifts through as much personal data as it deems necessary. While this result is certainly repugnant to the spirit of *Katz*, it would be the unfortunate consequence of faithfully applying the letter of the *Katz* doctrine.[139] The erosion of such expectations should not be taken to mean individuals lose access to their constitutional rights simply because society recognizes certain things are no longer private.[140] If the only bulwark against the encroachment of Fourth Amendment liberties is societal expectations of privacy, then the advent of the mass surveillance state is nigh inevitable.

---

enforcement official's aerial surveillance of the interior of a yard with a ten-foot fence was not an unreasonable search).

136. Gentithes, *supra* note 81, at 3–4.

137. Etzioni, *supra* note 115, at 419–20.

138. James Madison, *The Same Subject Continued: The Union as a Safeguard Against Domestic Faction and Insurrection from the New York Packet*, THE FEDERALIST PAPERS, NO. 10 (Nov. 23, 1787), http://avalon.law.yale.edu/18th_century/fed10.asp.

139. Even early commentators noted that accelerated technological innovations quickly undermined the protective intentions of the Warren Court. DiPippa, *supra* note 13, at 492.

140. Etzioni, *supra* note 115, at 420.

B. Positive Treatment of *Katz*

While *Katz* seems to be the doctrine that many academics love to hate, the decision is not without its defenders. Early commentary on the *Katz* doctrine suggested the decision was never meant to be a formulaic test, but instead should be applied "on a case-by-case basis"[141] in order to better conform to the changing realities of society.[142] Others suggest that *Katz* should not be understood as a radical departure from prevailing Fourth Amendment norms, but as a gentle shift to the "contemporary notions" of privacy rights.[143] Commentators have also praised *Katz* for rejecting the narrow, property-based focus of *Olmstead* in favor of a more liberal construction of privacy rights.[144]

Some of the above stated reasons might explain why, despite the repeated criticism of scholars, the *Katz* doctrine has enjoyed a storied history across more than fifty years of jurisprudence. Indeed, the Court has consistently upheld the constitutionality of the *Katz* doctrine, eschewing all academic alternatives proposed.[145] Institutional pressures might also explain the longevity of the *Katz* doctrine. The Supreme Court is predominantly focused on producing judicial decisions based on some conceptual framework that does not require development of onerous legal tests. Precedent is a powerful motivation. Even though the initial foundation is weak, the Supreme Court has to understand the *Katz* doctrine as an axiom of Fourth Amendment jurisprudence.[146] The Court is unlikely to dispose of the doctrine anytime soon.

---

141. John W. Boyd, *The Reasonable Expectation of Privacy*—Katz v. United States*, a Postscriptum*, 9 IND. L. REV. 468, 471 (1976); *see also* Winn, *supra* note 47, at 12 (suggesting the flexibility of the *Katz* doctrine is a strength because, rather than "dictat[ing] what a reasonable expectation of privacy is," the doctrine "provides the structure in which the debate can take place").

142. Boyd, *supra* note 141, at 475; Nicholas Matlach, Comment, *Who Let the Katz Out—How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in* Katz v. United State*s Will Fix It*, 18 COMMLAW CONSPECTUS 421, 424 (2010); Daniel T. Pesciotta, Comment, *I'm Not Dead Yet:* Katz, Jones*, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187, 244–45 (2012).

143. Boyd, *supra* note 141, at 473; *see also* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1306 (2002) (arguing that, originally, *Katz* was meant to protect the privacy of individuals by focusing on the results of the search, regardless of the method of collection).

144. Boyd, *supra* note 141, at 498; Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH L. REV. 143, 157–59 (2015).

145. Amsterdam, *supra* note 60, at 350–52.

146. *See* Kerr, *Technologies*, *supra* note 36, at 838 (noting the body of law surrounding the Fourth Amendment "reflects a relatively humble and deferential judicial attitude").

IV. TWO APPROACHES TO SOLVING THE EXPECTATIONS MORASS

Despite the persistence of the *Katz* doctrine, scholars have proposed numerous methods for re-imagining Fourth Amendment jurisprudence.[147] Two theories have recently enjoyed attention from the dissenting justices in *Carpenter*: the positive law theory[148] and property-based theory.[149] Both of these theories provide useful paradigms for examining the scholastic trends associated with Fourth Amendment jurisprudence. This Part will examine both theories, including their advantages and limitations. While both theories present compelling reasons for abandoning the *Katz* doctrine, neither lend themselves to an easily deployable test to replace the *Katz* doctrine.

A. Developing Positive Law Solutions

Some scholars have proposed adopting a positive law approach, which would evaluate government actions in light of what private citizens are allowed to do in similar circumstances.[150] The positive law model suggests that a search occurs whenever the government attempts to obtain information in a way that the law would otherwise prevent, except when the "government official has taken advantage of [some legal] exception" that exempts government officials from criminal liability.[151] While the Court's precedent since *Katz* has focused almost exclusively on privacy concerns, as the positive law advocates note, the central concern of the Fourth Amendment is actually "abuse of government power."[152] Drawing on the historical legal regime at the

147. For other proposed solutions to the various problems identified in *Katz*, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 17–20 (2007); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823 (2016); Casey, *supra* note 2, at 977; Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 37 (2018) [hereinafter Cloud, *Property*]; Colb, *supra* note 81, at 119; DiPippa, *supra* note 13, at 483; Heffernan, *supra* note 36, at 1; Kerr, *Technologies*, *supra* note 36, at 801; Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 313 (2015–2016); Luke M. Milligan, *The Real Rules of Search Interpretations*, 21 WM. & MARY BILL RTS. J. 1 (2012); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006).

148. Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting).

149. *Id.* at 2235 (Thomas, J., dissenting).

150. Baude & Stern, *supra* note 147, at 1821. Justice Gorsuch favors this theory. *Carpenter*, 138 S. Ct. at 2262–63 (Gorsuch, J., dissenting).

151. Baude & Stern, *supra*, note 147, at 1831.

152. *Id.* at 1828. *See also* Cloud, *Pragmatism*, *supra* note 53, at 295 ("The [F]ourth [A]mendment exists for the very purpose of enhancing individual liberty by constraining government power."); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1312 (2012)

time the Fourth Amendment was drafted, the positive law advocates note that, historically, private legal remedies were the only legal recourse citizens had for enforcing their Fourth Amendment rights to be secure from unreasonable searches and seizures.[153] Modern remedies such as the exclusionary rule simply did not exist.[154] By focusing on a positive law perspective, the Fourth Amendment can better concentrate on "what is distinctive about the government and what is distinctly dangerous about it."[155]

Although the positive law theory provides an interesting perspective on the Fourth Amendment, it ultimately cannot provide a completely accurate model for evaluating it. The positive law theory downplays the legitimate role the government has in enforcing the law. Police power is a constitutionally recognized authority granted to the State to promote "public safety, health, and morals."[156] When law enforcement officials act to enforce state criminal laws, they are taking actions to enforce legitimate state interests in promoting public welfare. Actions taken by private citizens are therefore not entirely analogous to the actions of a law enforcement officer. Conversely, citizens have a greater interest in limiting government intrusions into their affairs precisely because the government has a legal monopoly on the use of coercive force. An ordinary citizen asking intrusive questions about the contents of another citizen's car is inconsequential. A law enforcement officer asking identical questions carries with it the full force of the State.[157] Any comparison of law enforcement efforts to the actions of private citizens fails because it does not account for this power dynamic.

B. Modifying the Property-Based Approach

Consistent with the opinion of the late Justice Scalia, Justice Thomas advocates returning to a more property-focused Fourth Amendment jurisprudence.[158] According to the property theory, the Fourth Amendment defines the property interests of citizens by specifically

(arguing that the Fourth Amendment was concerned "not [with] privacy but liberty from undue government power").

153. Baude & Stern, *supra* note 147, at 1840–41.
154. *Id.*
155. *Id.* at 1848.
156. Lawton v. Steele, 152 U.S. 133, 136 (1894).
157. Re, *supra* note 147, at 323.
158. Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018) (Thomas, J., dissenting).

naming the person, the house, papers, and effects as protected areas.[159] Analysis of whether a search or seizure has occurred should therefore focus on whether the government has intruded on the property interests of the individual.[160]

Proponents of the theory point out that while the word "privacy" was not in the political vocabulary of the founding generation, they were well-versed in property rights theory.[161] The Fourth Amendment was an acknowledgement of already existing common law protections.[162] Property, as understood by the founding generation, encompassed broader notions than the modern conception of property.[163] Influenced by the Lockean theory[164] of property rights, the Founders understood that "rights and liberties were a person's property."[165] The Fourth Amendment, therefore, should be understood as a means of protecting one's right to be secure in their property against government intrusion on individual freedoms.[166]

While this approach has merit, the application of the traditional property-based theory requires more refinement. The property-based theory relies on notions long since abandoned by scholars and the Supreme Court. Although the Lockean theory of property conceptualized the rights of citizens as their property, modern pretensions about expansive privacy rights have obscured the connection between the exercise of an individual's rights and property. If the Court were to recover these property-based conceptions, the standard must be carefully crafted to avoid a wholesale retreat into

159. *Id.* at 2239; Cloud, *Property*, *supra* note 147, at 40–41.

160. *Carpenter*, 138 S. Ct. at 2239 (Thomas, J., dissenting).

161. Cloud, *Property*, *supra* note 147, at 42–43.

162. Kerr, *Technologies*, *supra* note 36, at 809 (finding that "a strong and underappreciated connection exists between the modern Fourth Amendment and real property law"). *See also* Donohue, *supra* note 12, at 1271 (arguing the Founders approached the rights in the Constitution as enumerations of pre-existing common-law rights).

163. As one commenter noted, the founding generation thought property included "all of those human rights, liberties, powers, and immunities that are important for human well-being, including: freedom of expression, freedom of conscience, freedom from bodily harm, and free and equal opportunities to use personal faculties." Laura S. Underkuffler, *On Property: An Essay*, 100 YALE L.J. 127, 129 (1990).

164. JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT § 123 (C.B. MacPherson ed., Hackett Publ'g Co. 1980) (1680). *See also* JACK RAKOVE, REVOLUTIONARIES: A NEW HISTORY OF THE INVENTION OF AMERICA 78 (2010) (explaining that John Locke understood that "[m]en did not merely *claim* their rights, but also *owned* them, and their title to their liberty was as sound as their title to the land or to the tools with which they earned their livelihood.") (emphasis in original).

165. Cloud, *Property*, *supra* note 147, at 43.

166. *Id.* at 75.

Olmstead's literalist application of the text of the Fourth Amendment.[167] To echo the criticism Justice Alito levied at the majority's decision in *United States v. Jones*, the Fourth Amendment does not hinge on a "technical trespass."[168] The Court needs to establish a standard that affords constitutional protection to the person even if their person, house, papers, or effects are not physically trespassed.

V. THE ALTERNATIVE: SEARCH AS A DIGITAL TRESPASS

Carpenter illustrates the untenability of continuing under the *Katz* doctrine. Nevertheless, the Fourth Amendment needs a test that does not resort to circular theories. While the positive law and property-based theories provide compelling principles for abandoning *Katz*, neither offer a clear, analytical test that can be readily applied to cases. This Part suggests the Court should adopt a digital trespass test to replace the *Katz* doctrine. By extending the legal principles briefly considered in *Kyllo* and *Jones*, the Court could use this digital trespass test to ground Fourth Amendment search and seizure analysis into more precise reasoning.

A. Outlining the Theory

A digital trespass doctrine would best serve the Fourth Amendment by developing robust protections for the person, and their house, papers, and effects. The new doctrine would combine the broader conception of property from the property-based theory and the limiting-government-action principle from the positive law theory. Essentially, the doctrine expands the traditional physical trespass theories by analogizing the digital realm to physical trespass. This new paradigm ought to evaluate three questions:

1. Does the technique used amount to an actual digital or physical trespass on an individual's person, house, papers, or effects?[169]

---

167. Wilkins, *supra* note 52, at 1088.

168. United States v. Jones, 565 U.S. 400, 423 (2012) (Alito, J., concurring).

169. *See* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. Rev. 1, 73–75 (2012) (discussing how the *Jones* trespassory test was a modest modification of Fourth Amendment rules in order to introduce larger doctrinal changes); Emas & Pallas, *supra* note 66, at 147 (explaining how Justice Scalia wanted to shift Fourth Amendment jurisprudence to a trespass doctrine over the *Katz* doctrine).

2. Would one be able to reasonably obtain the same type of information through non-technological means without searching the individual's person, house, papers, or effects?[170]

3. Would one reasonably be able to collect the same volume of data using a different non-technological means?[171]

The first question focused on the way data is collected. If the action would constitute a physical or digital trespass on the person, and their house, papers, or effects, then the inquiry ends because these actions are unreasonable searches or seizures of the person's property.[172] For example, consider *Kyllo* where law enforcement officers saw details of the home.[173] Such details could only be revealed by either physically trespassing on the property or digitally trespassing using the thermal image scanner.[174] In either instance, the law enforcement officials have "searched" the house. These actions would fail the first question in the digital trespass test.[175]

If the first question is answered in the negative, however, a court would proceed to the second question to consider whether the type of data collected could be obtained without a search of a person, their house, papers, or effects. Whereas the first question considers the means law enforcement used, the second question considers what information is obtained compared to how law enforcement could gather analogous information through a non-technological investigation. If a non-technological search could obtain the information only by searching the person's digital or physical property, then law enforcement's actions

170. Similar propositions have found their way into Fourth Amendment literature. DiPippa, *supra* note 13, at 514 (advocating a search test, which would consider objective factors to determine the reasonableness of a search based on the extent of information revealed and the consequences of revealing such information).

171. This question addresses one of the critical concerns of the majority in *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (determining that the actions of law enforcement yielded "an all-encompassing record of the [cell phone] holder's whereabouts"). Justice Alito also expressed similar sentiments in *United States v. Jones* when he observed "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." 565 U.S. 400, 430 (2012) (Alito, J., concurring).

172. *See also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (finding attempts to gain information through the use of advanced surveillance technology that reveal information otherwise "unknowable without physical intrusion" violate the Fourth Amendment).

173. *Id.* at 29–30.

174. *Id.* at 40.

175. While the majority in *Kyllo* did not explicitly hold that the use of a thermal imaging device should be understood as an electronic trespass, advocates of the property-based approach have suggested the Court extend the *Kyllo* precedent to cover all searches which are the "*functional equivalent of a trespass*." Cloud, *Property*, *supra* note 147, at 69 (emphasis in original).

would still be a trespass. If, after considering the first two questions, a court determines the practice is acceptable, it must finally evaluate the extent of data collected during the investigation.[176] Comprehensive searches that capture extensive records would be unacceptable, but limited collection of small amounts of data would be tolerable.

B. The Meaning of Property in the Digital Trespass Doctrine

The digital trespass doctrine takes a more expansive reading of property.[177] Although indiscriminately characterizing the right to be free from government intrusion as a property right in itself might be too generous, the Lockean property rights theory provides useful insights for how the Supreme Court ought to understand Fourth Amendment protections. Conceptualizing the rights protected by the Fourth Amendment in terms of property interests provides a language for understanding precisely what is protected and when exactly the government may intrude on those protections. The digital trespass theory, therefore, does not mechanically transpose the whole body of property and tort law onto the Fourth Amendment.[178] Rather, the digital trespass theory creates a conceptual reference point so that a court might better explicate the scope and limits of the doctrine. For instance, applying the digital trespass test to data stored on servers for social media sites could strain the property-based thinking of the new doctrine. Some major technology companies have developed business models dependent on collecting user data for the express purpose of selling that data to advertisers.[179] The user does not have a fully-

176. This third question along with the first would act as a limiting principle which addresses many of the Supreme Court's concerns about analogue tests mentioned in *Riley v. California*, 573 U.S. 373, 401 (2014). *See discussion infra* pt. V.D.

177. *See supra* pt. IV.

178. Justice Alito expressed frustration with Justice Scalia's formulation of the trespass test because he believes it introduces the legal intricacies of outdated legal precepts into the Fourth Amendment. *See* Florida v. Jardines, 569 U.S. 1, 18–22 (2013) (Alito, J., dissenting) (arguing how the function of a license under trespass law undermines Justice Scalia's analysis); United States v. Jones, 565 U.S. 400, 418–19 (2012) (Alito J., concurring) (calling it "unwise" to rely on "18th-century tort law"). This criticism misses the larger analytical point. Justice Scalia's reference to trespassory law does not impose the minutia of tort and property law on the Fourth Amendment. Rather, his reasoning uses property-based principles to inform how the right to be free from government intrusion should be conceptualized. *Jardines*, 569 U.S. at 8 (Justice Scalia explaining that "[c]omplying with the terms of that traditional invitation does not require fine-grained legal knowledge").

179. Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

developed property interest in the data stored on these sites because they do not own the data.[180] If the digital trespass doctrine required formal ownership, then most users would be without recourse if the government wished to obtain that data absent a warrant. However, the digital trespass doctrine considers the broader principles that inform the right to secure one's property from unreasonable government intrusion.

Content created in the digital world could be seen as "expressive property."[181] An individual has a constitutionally recognized interest in protecting their digital content because they have an interest in creating, maintaining, and controlling their own information. An individual need not have exclusive ownership of expressive content to assert a Fourth Amendment interest in securing it from government intrusion. An individual need only have a possessory interest reasonably related to the interests of an individual seeking to protect their person, house, papers, and effects. Using property concepts to ground the digital trespass doctrine provides clarity consistent with how the Court has understood the relationship between property interests and Fourth Amendment protections.[182]

In the property context, "effects" should be read liberally to include digital "effects" such as cell phone data, hard drives, data stored on servers, etc. Similarly, the data transmitted from a device ought to be conceptualized as an extension of a personal effect requiring at least some protection.[183] A cell phone is someone's personal effect as much as an email is analogous to someone's papers. This conception of digital technology as a personal effect, however, should not be pushed too far. Instead, the analogy should be limited. Data transmitted directly by the cell phone would be protected, but the protection would not extend to

180. Facebook, for instance, includes terms of service that grant the company ownership of data generated on their platform. *Id.*

181. *See also* Cloud, *Property*, *supra* note 147, at 56–58 (arguing that property should include "expressive property" such as the writings and ideas produced by individuals regardless of the medium).

182. Baude & Stern, *supra* note 147, at 1836 (explaining that the majority in *Jardines* and *Jones* were more interested in drawing conceptual parallels to property law than actually applying specific state laws related to property).

183. *See* Kerr, *Technologies*, *supra* note 36, at 835–37 (discussing how, despite the Court's limited use of the precedent, the rationales of *Kyllo* and *Karo* could be read broadly to establish more universal applications beyond just the home).

all information about the cell phone.[184] By focusing on securing digital property from unreasonable searches, the Court can more readily protect the freedoms of individual citizens.[185]

C. Applying the Digital Trespass Doctrine

The digital trespass doctrine would effectively replace the *Katz* doctrine. Rather than evaluate the Fourth Amendment on malleable notions of societal expectations of privacy, the digital trespass doctrine would focus on the proprietary interests of the individual. While this digital trespass test would replace the *Katz* doctrine, it would not supplant the common law trespassory doctrine.[186] When considering law enforcement actions in the digital world, courts should use the three-part framework explored in Part V. For non-technological investigations, however, the court should continue to use the common law trespass doctrine. Thus, the reasoning and holdings of *Kyllo*, *Jones*, and *Jardines* would remain undisturbed by this doctrine.

Pre-*Katz* decisions applying *Olmstead*, however, would no longer be good law.[187] The facts of *Olmstead* present a useful example of how the digital trespass doctrine should extend beyond the original constraints of the property regime. The officers began intercepting the phone conversations by wiretapping the phone line that extended past the physical space of the home.[188] While the Court held there was no "physical trespass,"[189] the officers did commit a digital—or technological—trespass. This action fails the first question in the digital trespass test. If law enforcement used a non-technological means of eavesdropping on the conversation, they would have physically

184. Thus, while data transmitted directly from the cell phone, including any CSLI or GPS data, is protected, business records about an individual's possession of a cell phone, such as terms of contract or billing statements, would not be protected.

185. *See generally* Casey, *supra* note 2, at 1025–27 (discussing how focusing on normative rights over privacy expectations better protects the fundamental interests in the Fourth Amendment).

186. In this regard, adopting the digital trespass doctrine would closely follow the reasoning articulated in *United States v. Jones*, 565 U.S. 400, 409 (2012) (saying the "*Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test") (emphasis added).

187. Olmstead v. United States, 277 U.S. 438, 466 (1928). The digital trespass doctrine would merely replace *Katz* and co-exist with the common-law trespassory test.

188. *Id.* at 456–57.

189. *Id.* at 457.

intruded into the petitioner's residence and therefore failed to pass the second question in the digital trespass test.[190]

The digital trespass doctrine would almost eliminate the third-party doctrine articulated in *Smith v. Maryland*. If a court were to evaluate the facts of *Smith* using the digital trespass test, it would first have to evaluate whether the installation of a pen register would amount to a digital trespass.[191] Obtaining information from a pen register would constitute a trespass onto the phone—a personal effect.[192] Although the phone company regularly collected phone numbers dialed, law enforcement officials obtained these numbers by intercepting data transmitted by the phone to the phone company.[193] In other words, law enforcement officials captured data from the phone and secured it for their own purposes. Here, even though analogous information is stored with the phone company, law enforcement used a method which trespassed on the individual's property. Thus, law enforcement use of the pen register would not be a reasonable search absent a warrant.

Even if the digital trespass doctrine does not make such actions a trespass covered under the first question, the second question makes it a digital trespass "in effect" because it reveals information not otherwise discoverable using non-technical means without searching someone else's property. The only other way to obtain the phone records without using a pen register would involve either physically trespassing in the home or obtaining the records from the phone company. While the majority in *Smith* found there is no expectation of privacy when someone knowingly discloses information to a third-party,[194] the digital trespass test would forbid law enforcement from seizing one individual's property for the purpose of incriminating another without some form of independent oversight. Absent a warrant to search the phone company's records, law enforcement could not justify such a trespass.

The digital trespass doctrine would not modify the outcome of *Carpenter v. United States*,[195] but it would provide a more consistent rationale for why collecting such information violates the Fourth

190. *Id.* at 456–57.
191. Smith v. Maryland, 442 U.S. 735, 740 (1979).
192. *Id.* at 741–42 (explaining the process of how the phone numbers are stored on pen registers).
193. *Id.* at 737, 742.
194. *Id.* at 743–44.
195. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

Amendment. Since the FBI obtained the records from phone companies, it did not digitally trespass on Carpenter's phone, thus passing the first question of the digital trespass test.[196] However, the FBI would have no other means of collecting 12,898 location points spanning more than 127 days through non-technological means without engaging in a digital trespass on Carpenter's phone.[197] Such actions would require a veritable army of officers working around the clock to carefully monitor the individual. Thus, the FBI's actions would fail both the second and third questions of the digital trespass test.[198] The digital trespass doctrine would provide a more consistent framework for applying the Fourth Amendment, avoiding the ambiguities inherent in the *Katz* doctrine without returning to the mechanical literalism of *Olmstead*.

D. Advantages of the Digital Trespass Doctrine Over *Katz*

While the *Katz* doctrine requires judges to grapple with vague notions like public opinion, the digital trespass test addresses readily understood property interests. Instead of relying on their own notions of societal expectations, judges will be able to evaluate whether the government trespassed on someone's property.[199] The digital trespass doctrine removes subjective social evaluations from decisions about constitutional rights.[200] Likewise, judges would no longer have to determine whether to use statistically valid survey results, or consider the inherent limitations of survey research, while crafting judicial decisions.[201] While analogizing Fourth Amendment property protections to the digital world requires some judicial flexibility, the

196. *Id.* at 2212.

197. *Id.*

198. Justice Alito's argument in *Carpenter* about the function of a subpoena to obtain the records, *id.* at 2247–54, would not factor into this analysis because the digital trespass doctrine considers the information collected, not necessarily what direct means the government uses to obtain the information. It is irrelevant whether law enforcement officials captured the CSLI data themselves or obtained it from a third-party. The FBI would not have reasonably been able to obtain that type of information—persistent location data—without dedicating significant resources to a round-the-clock surveillance team or searching another person's property.

199. The Court has already created a "firm but also bright" line constitutionally protecting the house from "sense-enhancing technology." Kyllo v. United States, 533 U.S. 27, 40, 45 (2001). The digital trespass doctrine can be seen as nothing more than a logical extension of *Kyllo*'s basic rationale to the remaining protected areas mentioned in the Fourth Amendment.

200. *See* Etzioni, *supra* note 115, at 419–20 (describing the disadvantages of defining constitutional rights on something malleable like expectations of privacy).

201. *See id.* at 416–19 (discussing the numerous analytical problems judges face when defining social expectations).

logic of the digital trespass doctrine provides a much more concrete, workable guideline than the *Katz* doctrine.[202]

The *Katz* doctrine is partially correct: the Fourth Amendment protects people.[203] But it also protects "houses, papers, and effects."[204] All of these constitutionally protected areas should be rigorously safeguarded. By analyzing Fourth Amendment protections under a property-based paradigm instead of a privacy rubric, the Court can readily articulate justifications that "assure[] preservation of [a] degree of privacy" more consistent with the protections of the Fourth Amendment.[205] Property provides a more readily accessible justification for evaluating new technology, which threatens to disrupt social expectations about privacy.[206] Leaving privacy to the subjectivity of the *Katz* doctrine, absent property guidance, diminishes both privacy and property interests of citizens. By focusing on property, the digital trespass doctrine provides more robust protection for both the privacy and property interests of citizens.[207] The doctrine, however, is not without its challenges.

E. Potential Challenges of the Digital Trespass Doctrine

To address modern concerns with technology, the digital trespass test requires some analogical reasoning.[208] Analogizing digital trespass to physical trespass requires that one views the Fourth Amendment as protecting individual liberties of citizens to secure their property against government intrusion, be it digital or physical property.[209] But this normative abstraction about the original meaning of the constitutional text can easily create unsophisticated myths about the historical

202. *See generally* Casey, *supra* note 2, at 1025–27 (discussing how focusing on the rights of the people to be secure from the government, rather than attempting to determine the normative expectations of privacy, better protects the fundamental interests in the Fourth Amendment).

203. Katz v. United States, 389 U.S. 347, 351 (1967).

204. U.S. CONST. amend. IV.

205. Kyllo v. United States, 533 U.S. 27, 34 (2001).

206. Kerr, *Technologies*, *supra* note 36, at 835 (examining how *Kyllo* and *Knotts* illustrate that "the Court has fashioned new rules in an effort to retain the traditional protections set by property law").

207. Cloud, *Property*, *supra* note 147, at 71–73 (explaining how privacy interests are best served by understanding Fourth Amendment protections in property-based terms).

208. The analogy, however, is not that distant from the original meaning of the Fourth Amendment. Kerr, *Technologies*, *supra* note 36, at 835 (noting how the property concerns in *Kyllo* and *Karo* address the "very core of traditional Fourth Amendment protections").

209. Ohm, *supra* note 152, at 1312.

purpose of the Fourth Amendment.[210] Considering the abstract principles of the Fourth Amendment de-coupled from the Amendment's historical context belies the Framers' understanding of the Constitution and reduces the Amendment to subjective interpretations.[211]

While concerns that the digital trespass test might succumb to a crude revisionist understanding of the Fourth Amendment are certainly well placed, the digital trespass doctrine seeks to remediate the same issues that the founding generation considered essential to the Fourth Amendment. As the founding generation sought to curb the government's infringement of citizens' property rights,[212] so too does the digital trespass test protect citizens from government intrusion onto their digital property. Thus, the digital trespass doctrine is not an exercise of re-constructing a mythical past but a realization of the original principles that informed the Fourth Amendment.[213] While the Framers certainly could not have anticipated the technological revolution of the twenty-first century, the digital trespass doctrine matches their concerns for preserving the liberty of individual citizens from government overreach.

Analogical reasoning can also become an exercise in futility. In *Riley v. California*, the Justices rejected an analogue test that would allow law enforcement to gather information from a digital medium if law enforcement would have been allowed to search a similar non-digital medium.[214] For example, the proposed analogue test would allow the government to search photos on a cell phone because law enforcement officials could also encounter a photo while searching in a wallet incident to an arrest.[215] The Court rejected this proposed analogue test for two reasons. First, the Court argues there is a fundamental difference between the quantity and quality of information in a digital search compared to pre-digital analogs. Encountering a photo in a wallet is a poor comparison to searching thousands of photos stored on a cell

210. Davies, *supra* note 15, at 740–41 (suggesting that attempts to apply the original meaning of the Fourth Amendment in a "completely changed social and institutional context" could only "subvert the purpose the Framers had in mind when they adopted the text").

211. *Id.* at 744–46.

212. *Supra* pt. IV.

213. *See* Baude & Stern, *supra* note 147, at 1843–44 (explaining the Founders would have understood that the meaning of the Fourth Amendment broadly concerned protecting property rights).

214. Riley v. California, 573 U.S. 373, 376 (2014).

215. *Id.*

phone.[216] Second, the Court thought such an analogue test would create significant guesswork about "which digital files are comparable to physical records."[217] The proposed analogue test would leave law enforcement and the courts to guess at how to apply the rule without providing effective principled guidance.[218]

The digital trespass doctrine, however, addresses the *Riley* Court's concerns about analogical comparisons. First, while the digital trespass doctrine does make similar comparisons between pre-digital and digital information, this comparison is not a stand-alone test but acts as a stop-gap against actions that might not technically constitute a digital trespass.[219] Under the digital trespass doctrine, law enforcement cannot escape the Fourth Amendment warrant requirement by showing that there is some non-digital version of the data they wish to obtain. Rather, they must address why the quality and quantity of data they collected should not be taken as an effective trespass. Second, by grounding the digital trespass test in property-focused analysis, the digital trespass doctrine provides an effective mechanism for comparing digital files to physical records. Unlike the test proposed in *Riley*,[220] the courts and law enforcement would not have to guess on how to extend the analogy. Instead, they would look to the possessory interests of the individual who held the digital property. Based on those possessory interests, the digital trespass doctrine would allow the individual to secure themselves from government intrusion onto their property. As such, the digital trespass doctrine provides the necessary principled guidance to avoid fruitless line-drawing expectations while providing a categorical

216. *Id.*
217. *Id.*
218. *Id.* (noting that such a test would "launch courts on a difficult line-drawing expedition").
219. For example, intercepting data transmitted from a cell phone or computer might not constitute a technical trespass, but it would be an effective trespass because law enforcement would not be able to obtain that type of information using non-technological means without trespassing on the individual's property—i.e., their phone or computer. *See also* Kyllo v. United States, 533 U.S. 27, 38–40 (2001) (discussing how a "functional equivalent of actual presence" test, if applied without distinctions between the type of details revealed, would be compatible with the majority ruling, which protects constitutionally-specified areas from sense-enhancing technological intrusion).
220. *Riley*, 573 U.S. at 376.

rule[221] that will facilitate predictable law enforcement practices as technology evolves.[222]

VI. CONCLUSION

In the twenty-first century, technology presents a unique challenge to the *Katz* doctrine. More than fifty years after the Warren Court dramatically proclaimed that "the Fourth Amendment protects people, not places,"[223] the Supreme Court is still puzzling through exactly how the law ought to realize the vision of the Warren Court. The conceptual and practical difficulties of attempting to divine what society is prepared to recognize as reasonable ensure that the problems introduced by *Katz* remain unmanageable.[224]

Far from abridging privacy concerns, the digital trespass doctrine offers a better means of protecting the privacy interests of individual citizens. By focusing on the rights of citizens to secure their property, both digital and tangible, from government intrusion, the digital trespass doctrine eliminates the subjective elements of the *Katz* doctrine in favor of more grounded concepts. While the digital trespass doctrine is not without challenges, the doctrine does provide more effective protection for citizens because it focuses on more readily understood concepts of property. Such precise inquiry avoids the ethereal, ever-evolving notions of privacy that individuals may or may not actually understand. By grounding the Fourth Amendment in more analytically sound concepts, the digital trespass doctrine can better adapt to twenty-first century challenges and secure the rights of the people to be free from unreasonable government intrusion.

221. *See id.* at 398–99 (noting that Fourth Amendment jurisprudence prefers categorical rules over ad-hoc approaches to increase predictability and ensure compliance with legal requirements).

222. *See* Maclin, *supra* note 60, at 70 (discussing how the Court typically reasons that "bright-line-rules are also meant to provide guidance" to law enforcement).

223. Katz v. United States, 389 U.S. 347, 351 (1967).

224. As Justice Thomas explained, "[u]ntil we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence." Carpenter v. United States, 138 S. Ct. 2206, 2236 (2018) (Thomas, J., dissenting).