St. Mary's Law Journal

Volume 51 | Number 1 Article 7

1-2020

Saving America's Privacy Rights: Why Carpenter v. United States Was Wrongly Decided and Why Courts Should Be Promoting Legislative Reform Rather Than Extending Existing Privacy Jurisprudence

David Stone
St. Mary's University School of Law

COMMENT

SAVING AMERICA'S PRIVACY RIGHTS: WHY *CARPENTER V. UNITED STATES* WAS WRONGLY DECIDED AND WHY COURTS SHOULD BE PROMOTING LEGISLATIVE REFORM RATHER THAN EXTENDING EXISTING PRIVACY JURISPRUDENCE

DAVID STONE*

* I gratefully acknowledge the assistance of Professor Gerald S. Reamey whose expertise was integral to this Comment; Professor L. Wayne Scott who helped me shape my loose ideas into a coherent and organized design; and my Comment Editor, Jordan H. Jentz, for providing helpful feedback and advice. Additionally, I thank the Volume 51 staff at the *St. Mary's Law Journal*, especially Research and Articles Editor, Louise Vollmer, who led the team that assisted me in getting this Comment ready for publication. I also thank my parents, David and Melissa Stone, as well as my grandmother, Carolyn Pruitt, for their unceasing encouragement and wisdom.

I. INTRODUCTION

In *Carpenter v. United States*,[1] the Supreme Court held that one has a reasonable expectation of privacy in cell site location information (CSLI).[2] In contrast to prior judicial direction,[3] law enforcement must now obtain a search warrant whenever they seek more than six days of CSLI from a cell phone service provider regarding a customer's whereabouts.[4] The Court reasoned that law enforcement violated the Fourth Amendment because the accumulated historical record of a citizen's movements is privacy-sensitive.[5] In so doing, the Court addressed the growing concern among Americans that the government can, and will, invade privacy through novel surveillance techniques.[6]

1. Carpenter v. United States, 138 S. Ct. 2206 (2018).
2. *Id.* at 2217.
3. *See In re* United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (deferring cellular data privacy questions to the voters); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (holding there is no reasonable expectation of privacy in CSLI).
4. *Carpenter*, 138 S. Ct. at 2212, 2217.
5. *Id.* at 2221.
6. *See id.* at 2219–20 (remarking on the dissent's failure to contend with the "seismic shifts in digital technology"); *see also* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016),

These concerns do not flow from unwarranted public hysteria. Federal agencies have reached the pinnacle of notoriety for singling out groups and individuals for surveillance and other harassment.[7] Generally applicable surveillance has generated a great deal of controversy as well.[8] Even when people realize their information is exchanged among multiple third parties, there is an understanding that information will be used according to the terms of service and not shared with a non-marketplace data broker.[9]

In many cases, third parties will stand up for user privacy when the government subpoenas customer information, but nondisclosure of user data is not guaranteed.[10] Until *Carpenter*, a cell phone user had no right to challenge a subpoena of CSLI because the data was said to belong to the service provider.[11] Thus, the user is at the mercy of the third-party service provider. Law enforcement has the element of surprise against the unwitting user (investigated party) who is not necessarily entitled to know—and even less likely to become apprised—of a request to sift through the

https://www.apple.com/customer-letter/ [https://perma.cc/J5PZ-88NG] (highlighting consumer concerns should Apple comply with FBI demands to produce surveillance software).

7. *See* Peter Fenn, Opinion, *Time to Clean House at the CIA*, U.S. NEWS (Aug. 1, 2014, 11:10 AM), https://www.usnews.com/opinion/blogs/peter-fenn/2014/08/01/fire-cias-john-brennan-after-senate-spying-scandal [https://perma.cc/K7EJ-FWV3] (chronicling the efforts of Senators Udall and Wyden to curb the CIA after the agency lied about spying on Congress); Editorial, *The IRS Targets Conservatives*, WALL ST. J., May 11, 2013, at A14 (discussing IRS harassment of conservative non-profit organizations); S. REP. NO. 94-755, at 12–18 (Comm. Print 1976), (exposing the FBI's domestic surveillance and harassment of advocacy groups and civil rights leaders, media manipulation, threatening of controversial professors and writers, and reading American mail supplied by the CIA); *cf.* Memorandum from Michael Horowitz, Inspector Gen., Dept. of Justice, to Christopher Wray, Dir., Fed. Bureau of Investigation 1 (Sept. 25, 2017) (describing "systemic issues" within the FBI such as multiple failed polygraph tests).

8. *See* ACLU v. Clapper, 785 F.3d 787, 794 (2d Cir. 2015) (detailing the privacy concerns of the ACLU in the bulk collection of metadata on nearly all Americans); Eyder Peralta, *NSA Ends Sept. 11-Era Surveillance Program*, NAT'L PUB. RADIO (Nov. 29, 2015, 2:09 PM), https://www.npr.org/sections/thetwo-way/2015/11/29/457779757/nsa-ends-sept-11th-era-surveillance-program [https://perma.cc/4H7L-ZUHB] (reporting the demise of bulk metadata collection amid public privacy outcry).

9. *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (opining it may be time to reconsider the notion that one cannot have a reasonable expectation of privacy in information conveyed to third-parties for limited purposes).

10. *See* Cook, *supra* note 6 (refusing to build a surveillance backdoor into iPhones for the FBI).

11. *See Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting) (denying a defendant has a legal interest in third-party-owned business records); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (discussing the government's ability to subpoena a third-party in possession of records an individual knowingly exposes to the third-party).

user's bank records, phone metadata, and search queries.[12] In contrast to searches of buildings, objects, or persons, the user will not have even the slightest opportunity to destroy evidence of criminal activity.[13] While no one questions the probative value of CSLI, there is a growing consensus that current privacy law is inadequate. Some jurists have suggested that the third-party doctrine, under which a person has no expectation of privacy in information conveyed to another, should be relaxed to permit the expansion of privacy rights.[14]

With this power and leverage comes the necessity of discipline and oversight in law enforcement and other government agencies. Unfortunately, it is difficult to stop invasions of privacy before the damage is effected.[15] Where surveillance techniques are unduly intrusive or occur over an extensive time period, many, including a plurality of the Supreme Court, believe such abusive state action should be proscribed by the Fourth Amendment.[16] Under this theory, during a criminal prosecution, the exclusionary evidence rule proscribes the admission of evidence procured through an unreasonable search, and discourages law enforcement from trying to obtain information without a warrant.[17]

---

12. *See* 18 U.S.C. § 2705(b)(3) (2012) (providing law enforcement with the ability to obtain a gag order against a computing service when customer communications are subpoenaed and where denial may result in the destruction of evidence); 31 U.S.C. § 5318(g)(2) (forbidding banks from notifying customers whose transactions have been reported to authorities as suspicious); *see also* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 86–89 (2017) (demonstrating the frequency at which the third-party doctrine is cited to obtain customer information from banking institutions and companies).

13. *See* United States v. Scully, 108 F. Supp. 3d 59, 86 (E.D.N.Y. 2015) (approving nondisclosure order pursuant to 18 U.S.C. § 2705(b) because disclosure would potentially jeopardize an ongoing government investigation).

14. *See* Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 95 (1974) (Marshall, J., dissenting) (refusing to adopt a "wooden" version of the Fourth Amendment that permits the government to circumvent search warrants for patron's bank records through a subpoena).

15. *See* 42 U.S.C. § 1983 (creating a tort for deprivation of constitutional rights by law enforcement); Mapp v. Ohio, 367 U.S. 643, 658–59 (1961) (mandating that evidence procured through a Fourth Amendment violation be excluded from evidence).

16. *See* United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J. concurring) (disagreeing with the proposition that secrecy is a prerequisite to enjoying privacy); *id.* at 429–31 (Alito, J., concurring) (concluding new non-physical surveillance technologies justify extending the Fourth Amendment to proscribe long-term surveillance without a warrant); *cf.* Kyllo v. United States, 533 U.S. 27, 40 (2001) (rejecting the government's contention that searching with a thermal imaging device that does not physically penetrate a home is outside the purview of the Fourth Amendment).

17. *See* Weeks v. United States, 232 U.S. 383, 398–99 (1914) (reversing a conviction in federal court based on evidence acquired through an illegal search and seizure).

Subscribers to this school of thought applauded when the Court announced its decision to extend Fourth Amendment protections to CSLI, but it remains to be seen whether this extension was proper as a matter of law. In extending the Fourth Amendment's coverage to Mr. Carpenter's CSLI, the Court reasoned that although the third-party doctrine usually precludes a reasonable expectation of privacy in records created and owned by third parties, CSLI data presents peculiar challenges to an individual's privacy rights in his physical movements.[18] The Court drew a line between CSLI data and the subpoena of bank records and telephone call metadata as areas in which one does not have a reasonable expectation of privacy.[19]

The Court's unexplained delineation recalls to mind a number of Chief Justice Roberts's other decisions which have pushed legal boundaries in a contrarian manner.[20] *Carpenter* should have been a straightforward case,[21] as information owned by a third-party is normally accessible via subpoena *duces tecum*.[22] Alternatively, the subpoena of Mr. Carpenter's CSLI was not a search within the meaning of the Fourth Amendment under either the reasonable expectation of privacy test (REOP test) or traditional trespass analysis.[23] Yet, *Carpenter* represents a watershed moment[24] in the legal history of the Fourth Amendment because it radically departs from three legal doctrines and creates a confusing and unworkable test. While the Court attempted to protect the average American's normative

18. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (blocking unlimited access to CSLI due to the "deeply revealing nature of CSLI").

19. *Id.* at 2216–19.

20. *See* Elonis v. United States, 135 S. Ct. 2001, 2013–14 (2015) (refusing to completely answer the question of what minimum level of culpability will sustain a conviction for terroristic threats and chiding Justices Alito and Thomas for their concern that Chief Justice Roberts potentially made the job of circuit courts more confusing); King v. Burwell, 135 S. Ct. 2480, 2490, 2495–96, (2015) (clarifying that "state" under the Affordable Care Act does not mean one of the United States, while also complicating the two-step *Chevron* doctrine); Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 589 (2012) (upholding a law mandating the purchase of health insurance because the term "penalty" actually meant tax).

21. *Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting).

22. *See* Donovan v. Lone Steer, Inc. 464 U.S. 408, 415 (1984) (declaring the validity of subpoenas for corporate books and other records "settled" law).

23. *See Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting) (explaining that even if it was a search, it was not an "'actual search' controlled by the Fourth Amendment's warrant requirement." (quoting majority at 2221)).

24. Daniel Solove, *The Supreme Court on Smart Phones: An Interview of Bart Huffman About Law and Technology*, LINKEDIN (Sept. 23, 2018) https://www.linkedin.com/pulse/supreme-court-smart-phones-interview-bart-huffman-law-daniel-solove [https://perma.cc/UJK6-ZQJZ] [hereinafter Solove].

expectation of privacy, the Court instead, in a result-oriented decision, reached beyond a fair exegesis of the Fourth Amendment and precedent to provide only modest privacy protection under the bright-line rule that requesting less than seven days of CSLI without a warrant does not run afoul of the Constitution.[25]

This Comment will address why *Carpenter* should have come to a different conclusion under the three aforementioned legal frameworks and seeks to provide the proper course for the Court to follow in order to both correctly interpret the law and promote the expansion of privacy protection. This Comment also takes the opportunity to reconsider the *Katz v. United States*[26] line of cases that led the *Carpenter* Court to reach its decision. If *Carpenter* and its *Katz*-jurisprudence predecessors incorrectly interpreted the law and insufficiently served the privacy interests for which they were created, the time is nigh to resolve privacy law, an area that characteristically lags behind the times.[27] As will be discussed in greater detail, the Court's historical attempts to patch the Fourth Amendment inadequately comport with the normative expectation of privacy held by the public. It follows that constitutional and statutory change is the proper remedy to the problem of privacy in the digital era.

The *Carpenter* test may one day be relegated to abstract theory, rarely applied, much like the establishment clause test in *Lemon v. Kurtzman*.[28] In the interim, however, the metaphorical floodgates of litigation are open, and law enforcement, jurists, and even *lawyers* have little guidance to ascertain whether information owned by a third party is protected by the Fourth Amendment. The ultimate question in future Fourth Amendment cases addressing third-party-owned information will be whether the information is more like CSLI data or other forms clearly excepted from the

25. As will be discussed *infra* Part III.A, one does not normally have an expectation of privacy in information belonging to third parties, but even if it does, the Supreme Court does not clarify why six days is the magic number. In a robbery case, like the one in *Carpenter*, the probative value of six days of information would likely be outweighed by the privacy intrusion if the suspect was far away from the crime scene on the day he was suspected of committing the crime. In such a scenario, one day is the focus, and the other days become potentially relevant only if the first day's records are inculpatory.

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

27. *See* Solove, *supra* note 24 ("[T]he Court struggles with how to incorporate the dominating characteristics of today's information technology within the doctrines of Constitutional law.").

28. Lemon v. Kurtzman, 403 U.S. 602, 613 (1971); *see also* Van Orden v. Perry, 545 U.S. 677, 686 (2005) (noting that within two years of the *Lemon* test's creation, the Court recognized the test factors only as signposts and otherwise declined to apply the test).

scope of the Fourth Amendment in prior cases.[29] This question is the blurry line drawn by the Court, but that is the road paved by *Carpenter*.[30]

II. A HISTORY OF THE FACTS AND LAW LEADING TO *CARPENTER*

A. *A Summary of the Facts in* Carpenter

The *Carpenter* case arose out of an interstate robbery spree ironically involving cell phone stores.[31] An accomplice to the criminal enterprise identified Mr. Carpenter as one of the robbers and provided Mr. Carpenter's cell phone number to the authorities.[32] Law enforcement then applied for a subpoena under the Stored Communications Act (SCA)[33] for Mr. Carpenter's CSLI.[34] To obtain a subpoena under the Act, the authorities only had to demonstrate specific and articulable facts indicating reasonable grounds that the information sought was relevant to a criminal investigation.[35]

The authorities met the burden of proof for the subpoena, a standard less burdensome than probable cause,[36] and subsequently acquired several months' worth of Mr. Carpenter's CSLI.[37] Although CSLI data is generally not as precise as GPS data, the information derived can prove that an individual was within several miles of a site covered by a cellular tower.[38] In Mr. Carpenter's case, his cell phone pinged the cell towers near the location of four of the robberies.[39] Because CSLI data provides a window into the general area of an individual's location at a particular time,[40] law enforcement was able to track all of Mr. Carpenter's movements during the

29. Carpenter v. United States, 138 S. Ct. 2206, 2234 (2018) (Kennedy, J., dissenting).

30. *Id.*

31. *Id.* at 2212 (majority opinion).

32. *Id.*

33. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

34. *Carpenter*, 138 S. Ct. at 2212.

35. § 2703(d), *declared unconstitutional in part by Carpenter*, 138 S. Ct. at 2221 ("[T]he Government must generally obtain a warrant supported by probable cause before acquiring [CSLI].").

36. *See Carpenter*, 138 S. Ct. at 2221 (recognizing the Stored Communications Act only requires evidence pertinent to an ongoing investigation rather than "some quantum of individualized suspicion" under a probable cause standard (quoting United States v. Martinez–Fuerte, 428 U.S. 543, 560–61 (1976))).

37. *Id.*

38. *See id.* at 2226 (Kennedy, J., dissenting) (describing the degree to which CLSI pinpoints an individual's location).

39. *Id.*

40. *Id.* at 2217 (majority opinion).

timeframe of the robberies.[41] The cumulative data also revealed the frequency with which Mr. Carpenter visited particular areas.[42] Based on the circumstantial evidence, Mr. Carpenter was arrested and later convicted.[43]

B. *Three Approaches the Supreme Court Could Have Used in* Carpenter

The Court had three approaches it could have used to decide *Carpenter*.[44] The threshold Fourth Amendment question is whether a search or seizure has occurred.[45] The easiest approach to resolve the case would have been under the traditional subpoena *duces tecum* analysis.[46] The alternatives for ascertaining the legality of searches are the trespass test[47] and the REOP test.[48] In the end, the Court chose a hybrid version of the REOP test that emphasized the novelty of recovering an individual's CSLI data through the issuance of a subpoena.[49]

Before one even considers the thorny question of searches in *Carpenter*, it is important to consider the distinction between subpoenas and searches.[50] In his dissenting opinion in *Carpenter*, Justice Alito posits that, while subpoenas are subject to some Fourth Amendment limitations, they are categorically different from searches.[51] Searches are much more invasive and require probable cause, while subpoenas are constructive searches subject to less judicial scrutiny.[52] Subpoenas follow the common law

41. *Id.* at 2226 (Kennedy, J., dissenting).

42. *Id.* at 2212–13 (majority opinion).

43. *Id.* at 2213.

44. *See id.* at 2257–60 (Alito, J., dissenting) (discussing the three tests previously used in Fourth Amendment jurisprudence).

45. *See* United States v. Jeffers, 342 U.S. 48, 51 (1951) (restating the Fourth Amendment prohibition on "unreasonable" searches and seizures).

46. *See Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting) (urging the Court to uphold traditional subpoena analysis and "more than a century of Supreme Court precedent.").

47. *Cf.* On Lee v. United States, 343 U.S. 747, 751–54 (1952) (declining to extend Fourth Amendment protections under a claim of trespass by eavesdropping because the federal agent did not physically enter petitioner's business by force, unwilling submission to authority, or without express or implied consent).

48. *See, e.g.*, Byrd v. United States, 138 S. Ct. 1518, 1522 (2018) (conceptualizing the reasonable expectation of privacy as a logical extension of property law's "right to exclude others").

49. *See Carpenter*, 138 S. Ct. at 2222 (majority opinion) (placing limitations on subpoenas where a suspect has a legitimate privacy interest in the information sought).

50. *Cf.* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 204–11 (1946) (recognizing the confusion between the distinct areas of actual searches and constructive searches via subpoena *duces tecum*).

51. *Carpenter*, 138 S. Ct. at 2256 (Alito, J., dissenting).

52. *Id.* at 2247.

understanding that a court has a right to any useful evidence.[53] The case could have been decided under the law governing subpoenas before diving into the depths of the Fourth Amendment search doctrine.[54] Nevertheless, the Court declined to base its judgment on the differences between subpoenas and searches.[55]

C. *A History of Fourth Amendment Search Doctrine*

Carpenter is the first of its kind in Fourth Amendment jurisprudence. To understand this case, one must first explore the history of this Amendment and cases interpreting it over the years. In common parlance today, the Fourth Amendment is the point of reference every time one invokes the right to privacy, but the extent to which this is true is a matter of debate.[56]

For much of America's history, few cases have addressed the Fourth Amendment's implications or even its provenance.[57] The first serious study of the Amendment occurred in the post-Civil War Era in *Boyd v. United States*,[58] which narrated the history leading up to its enactment.[59] In the eighteenth century, agents of the British monarchy were notorious for searching the houses, papers, and personal effects of its subjects using general warrants.[60] This generated a public outcry

53. Blair v. United States, 250 U.S. 273, 279–82 (1919) (reciting a litany of cases proving the longstanding validity of subpoenas under the common law and quoting Lord Bacon as remarking "[a]ll subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery."); *see also* Amey v. Long [1808] 103 Eng. Rep. 653, 653; 9 East 472, 473 (acknowledging the subpoena's compulsory nature and lawful effect); *cf. Carpenter*, 138 S. Ct. at 2249 (Alito, J., dissenting) (pointing to the Judiciary Act of 1789 as codifying the courts ability to compel useful evidence from parties).

54. *See Carpenter*, 138 S. Ct. at 2256–57 (Alito, J., dissenting) ("For over a hundred years, we have understood that holding subpoenas to the same standard as actual searches and seizures 'would stop much if not all of investigation in the public interest at the threshold of inquiry.'" (quoting Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 213 (1946))).

55. *Id.* at 2221–22 (majority opinion).

56. *Cf. id.* at 2243–44 (Thomas, J., dissenting) (reiterating the unfamiliar territory of technology and whether invoking the Fourth Amendment is reasonable in such circumstances).

57. *See* ERWIN N. GRISWOLD, SEARCH AND SEIZURE: A DILEMMA OF THE SUPREME COURT 2 (1975) ("Except for the *Boyd* case, virtually no search and seizure cases were decided by the Supreme Court in the first 110 years of [the United States'] existence under the Constitution, that is, up to the year 1900.").

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

59. *Id.* at 624–30.

60. *Id.*

throughout the British Empire.[61] Particularly in Colonial America, the Crown often granted general search warrants known as writs of assistance to its officials, especially customs officers.[62] The cost of the Seven Years' War meant that the American colonies would be managed under direct-rule to a greater extent than in previous years.[63] The Crown turned to its colonies for tax revenue.[64] The warrants were indefinite and allowed minor officers of the British Empire to invade the property interests of the public at will.[65] Each writ of assistance lasted for the life of the King and expired shortly after his death.[66]

Searches then, as they are now, could be considerably invasive and even destructive.[67] The English common law resisted the search and seizure tactics of early law enforcement against dissident voices and other perceived enemies of the Crown.[68] Joseph Story wrote that the Fourth Amendment was the culmination of longstanding common law rights against unreasonable searches and seizures which the King at every opportunity sought to destroy.[69] The people of the British Empire, including the American colonists, were infuriated by the abridgment of their property rights.[70] The instigating actions of British officials not only led to the Fourth Amendment barring unreasonable searches and seizures, but also to

61. *See id.* at 625 (narrating James Otis's case against writs of assistance, one of the final straws leading to revolution in America); Entick v. Carrington [1765] 95 Eng. Rep. 807, 818; 2 Wils. K.B. 275, 292 (declaring the secretary of state's general warrant in the name of the King to search for libelous materials null and void).

62. BRUCE A. NEWMAN, AGAINST THAT "POWERFUL ENGINE OF DESPOTISM": THE FOURTH AMENDMENT AND GENERAL WARRANTS AT THE FOUNDING AND TODAY 2 (2007).

63. Jeff Wallenfeldt, *Salutary Neglect*, ENCYCLOPAEDIA BRITANNICA (Mar. 10, 2015), https://www.britannica.com/topic/salutary-neglect#accordion-article-history [https://perma.cc/H3VG-QRYF].

64. *Id.*

65. NEWMAN, *supra* note 62, at 2.

66. *Id.*

67. *See* Entick v. Carrington [1765] 95 Eng. Rep. 807, 807–08; 2 Wils. K.B. 275, 275–76 (describing four hours of defendants breaking locks and rifling through boxes, drawers, and chests).

68. *See* Semayne's Case (1604) 77 Eng. Rep. 194, 195; 5 Co. Rep. 91 a, 91 b (reciting the English principal that a man's house is his castle and requiring the sheriff to knock on the door and announce a search prior to breaking and entering); NEWMAN, *supra* note 62, at 5–7 (discussing the common law customs of the English people that defied the powers of the monarchy).

69. JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 748 (1833).

70. NEWMAN, *supra* note 62, at 2–3.

the Third Amendment[71] proscribing the quartering of soldiers in the home.[72]

The Fourth Amendment encompasses a number of protections apart from privacy.[73] For example, highway patrolmen may not unreasonably seize a driver's Ford F-150. In this example, there is no privacy violation, but the driver has endured an offense to his constitutional rights by the "seizure" of his chattel.[74] The Fourth Amendment does not explicitly incorporate privacy,[75] although *Boyd* certainly considered the "privacies of life" important to the founders.[76] Privacy can be viewed as one component of property rights.[77] Paramount among property rights is the ability of an owner of something to exclude others from using it or interfering with said use.[78] Justice Black believed the right to privacy under the Fourth Amendment extended only insofar as property rights are concerned.[79]

Until the late 1960s, the property rights approach governed Fourth Amendment jurisprudence.[80] Under the property rights paradigm, the test for a Fourth Amendment search was whether the government had trespassed upon "persons, houses, papers or effects."[81] Modern proponents of this viewpoint include originalists such as the late

71. U.S. CONST. amend. III.

72. Engblom v. Carey, 677 F.2d 957, 966–67 (2d Cir. 1982) (Kauffman, J., concurring in part and dissenting in part).

73. *See* United States v. Mendenhall, 446 U.S. 544, 551 (1980) (explaining the Fourth Amendment protects a person from even a brief detention by law enforcement without cause).

74. *See* Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting) ("The average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and by stealth.").

75. *Id.* at 486–87 (Goldberg, J., concurring).

76. Boyd v. United States, 116 U.S. 616, 630 (1886).

77. *See* Carpenter v. United States, 138 S. Ct. 2206, 2239 (2018) (Thomas, J., dissenting) (observing privacy rights in the eighteenth century "were understood largely in terms of property rights." (quoting Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 42 (2018))).

78. *See* Dickman v. Comm'r, 465 U.S. 330, 336 (1984) (esteeming the use of property "to the exclusion of others" as the keystone of property rights (quoting Passailaigue v. United States, 224 F. Supp. 682, 686 (M.D. Ga. 1963))).

79. *See* Katz v. United States, 389 U.S. 347, 374 (1967) (Black, J., dissenting) (opining the Fourth Amendment protects privacy only to the degree it protects property interests).

80. *See* JAMES J. TOMKOVICZ & WELSH S. WHITE, CRIMINAL PROCEDURE: CONSTITUTIONAL CONSTRAINTS UPON INVESTIGATION AND PROOF 4–5 (8th ed. 2017) (describing the erosion of consensus regarding the proper Fourth Amendment search test after 1964).

81. *E.g.*, Florida v. Jardines, 569 U.S. 1, 5–6 (2013).

Justice Scalia and Justice Thomas.[82] This test is appealing in its direct link to the Fourth Amendment text:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[83]

Two immediate questions then follow under the trespass analysis: what is protected by the Fourth Amendment, and who may assert the right against unreasonable searches? These questions precede whether a search is even unreasonable—a fact-intensive process that requires a case-by-case analysis.[84] In analyzing the categories protected by the Fourth Amendment, "person" is hardly difficult to define as it refers to one's body.[85] "House," on the other hand, presents an intermediate level of difficulty. A house encompasses more than just the physical area beneath a roof and walls.[86] Thus, it is vague as to how far this protective area extends under the Fourth Amendment.[87]

The area just beyond the structure of the home is called the "curtilage," which extends for a reasonable distance away from the home.[88] It includes gardens around the home, the front porch, and nearby areas for parking vehicles.[89] These areas of the home are protected from searches to the extent that the plain view doctrine is not already implicated.[90] Subject to the customs of the land or other implied invitation, certain areas of the

82. Minnesota v. Carter, 525 U.S. 83, 91–92 (1998) (Scalia, J., concurring).

83. U.S. CONST. amend. IV.

84. GRISWOLD, *supra* note 57, at 13.

85. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 375–76 (2009) (holding a strip search, without probable cause, violates the right to be secure in one's person against unreasonable searches).

86. *See* Oliver v. United States, 466 U.S. 170, 180 (1984) (explaining a house includes the land immediately surrounding the home).

87. *See id.* at 182 (admitting no factor or set of factors is decisive in ascertaining whether something is part of the curtilage).

88. *See id.* at 180 ("[T]he curtilage is the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life . . . .'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

89. Collins v. Virginia, 138 S. Ct. 1663, 1675 (2018); Florida v. Jardines, 569 U.S. 1, 3–6 (2013).

90. *See* California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (clarifying anything in plain view is not protected by the Fourth Amendment even if it is done in or around the home).

curtilage may be welcome for law enforcement to visit, but no more than custom would allow, absent exigent circumstances.[91] While curtilage ends at a reasonable distance from the home, under the traditional trespass doctrine, open fields were not protected by the Fourth Amendment because they were not considered part of the home or any of the remaining enumerated situses.[92] These days, open fields remain unprotected for different reasons, namely that one simply cannot have a reasonable expectation of privacy in a field.[93]

Papers and effects are seemingly the most difficult of the enumerated Fourth Amendment protections to measure under the traditional trespass doctrine. Effects encompass virtually all chattels,[94] but how does one handle intangible or exchanged information in the digital era?[95] Technology alone does not present much difficulty for legal analysis under the original search jurisprudence, but it has presented problems for normative expectations of privacy.[96] The third-party doctrine should not be taken too seriously as one may have some privacy rights in papers conveyed to others in certain situations.[97] One can analogize email to papers, and the law of this country is evolving toward a consensus on this

91. *Jardines*, 569 U.S. at 8; Kentucky v. King, 563 U.S. 452, 469 (2011).

92. *Oliver*, 466 U.S. at 183–84; Hester v. United States, 265 U.S. 57, 59 (1924).

93. *See Oliver*, 466 U.S. at 184 (affirming the open fields doctrine as consistent with reasonable expectations of privacy).

94. *See* United States v. Place, 462 U.S. 696, 700–07, 710 (1983) (concluding the detention of a persons baggage for ninety-minutes is an unreasonable seizure of personal effects); United States v. Chadwick, 433 U.S. 1, 12 (1977) (holding automobiles are personal effects), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565 (1991); Maureen E. Brady, Comment, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 948–51 (2016) (assuming from the case law that "effects" encompass all personal property).

95. In some cases, the Court has treated some kinds of warrantless searches differently based on the source of information. For example, the Court determined that warrantless searches of cell phones seized from an arrestee implicates greater privacy interests because the information inside a cell phone is quantitatively and qualitatively different than other effects. Riley v. California, 573 U.S. 373, 393–97 (2014). Following *Katz*, it is far from clear how helpful these *sui generis* cases will be in the long run. *See* Minnesota v. Carter, 525 U.S. 83, 91, 97–98 (1998) (Scalia, J., concurring) (expressing concern that the reasonable expectation of privacy test (REOP test) is "fuzzy," "self-indulgent," and not warranted in the text of the Constitution).

96. *See* Susan Freiwald & Stephen Wm. Smith, Comment, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 223–27 (2018) (observing broad usage of the third-party doctrine prior to *Carpenter* to conclude that one has no expectation of privacy in information held by third parties).

97. *See Ex parte* Jackson, 96 U.S. 727, 733–37 (1877) (forbidding postal workers from opening and reading letters without a warrant).

matter.[98] The problem is that much of the information accompanying the use of chattels in the modern era creates a risk of privacy exposure and does not fit neatly into one's constitutionally protected categories, such as papers or effects.[99] Furthermore, there is still an ongoing debate as to whether one loses a total expectation of privacy once electronically stored information is passed to a bailee.[100]

The debacle of chattels generating risks to privacy is the sort of trouble Mr. Carpenter became entangled in. Although phone conversations are intangible and historically unprotected by the trespass doctrine,[101] telephone calls create metadata, which can be tracked.[102] Mr. Carpenter's cell phone generated multiple connections to cell towers everywhere he went, leading law enforcement to become knowledgeable of his whereabouts.[103] These issues will be discussed in greater detail momentarily, but the next area for consideration is who may assert the protections of the Fourth Amendment.

Historically, the issue of standing placed a number of constraints on who could assert a Fourth Amendment claim.[104] The Fourth Amendment codified many common law understandings, such as the English notion that one's home is one's sacred and inviolable castle that did not extend to

98. *See Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J., dissenting) ("Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted . . . ."); United States v. Warshak, 631 F.3d 266, 284–86 (6th Cir. 2010) (holding emails are like letters and subject to Fourth Amendment protection); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (recognizing emails as conceptually indistinguishable from letters and conferring Fourth Amendment protection upon them).

99. *See Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting) ("[This case] should turn, instead, on *whose* property was searched.") (emphasis in original).

100. *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (opining it may be time to reconsider the notion that one cannot have a reasonable expectation of privacy in information conveyed to third parties for limited purposes).

101. Olmstead v. United States, 277 U.S. 438, 465–66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

102. Metadata is defined as "secondary data that organize, manage, and facilitate the use and understanding of primary data." *Metadata*, BLACK'S LAW DICTIONARY (11th ed. 2019). The very nature of this type of data imputes the pernicious effect of CSLI as an evidentiary tool in the modern age. *Cf. Carpenter*, 138 S. Ct. at 2212 ("While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections."); Smith v. Maryland, 442 U.S. 735, 742 (1979) (discussing how the government can track telephone calls).

103. *See Carpenter*, 138 S. Ct. at 2212 (noting the government catalogued 12,898 location points of Mr. Carpenter's movements).

104. Minnesota v. Carter, 525 U.S. 83, 94 (1998) (Scalia, J., concurring).

strangers and other visitors.[105] This is not to say that, under the traditional trespass doctrine, only the owner of a fee simple absolute could assert the Fourth Amendment.[106] Indeed, apartment tenants, hotel guests, family members living at a residence, and even overnight house guests could assert Fourth Amendment protections.[107]

The reason for broaching the subject of imputed Fourth Amendment protections is that modern cases involving privacy often involve contractual relationships.[108] For example, a user of a social media platform has a contract called the "terms of service."[109] In exchange for advertising, the user is entitled to the platform's services, and each of the parties agrees to follow the terms of service.[110] Usually, such terms of service include limits on how much user data is collected.[111] For example, Facebook data is supposed to be anonymized before it is sold to consumers.[112] In theory, advertisers have no control over information that could specifically identify users.[113]

In the social media example, the question arises as to what role, if any, contractual relations play in creating Fourth Amendment protections against non-trespassory government intrusions. *Katz v. United States* appears to echo this when Justice Stewart remarked that the user of a telephone booth has an expectation of privacy because he has paid the toll and shut the door.[114] If a person has a contractual relationship with a third-party

105. *See* Semayne's Case (1604) 77 Eng. Rep. 194, 198; 5 Co. Rep. 91 a, 93 a ("[T]he house of any one is not a castle or privilege but for himself . . . .").

106. *Carter*, 525 U.S. at 95 (Scalia, J., concurring); *see* Chapman v. United States, 365 U.S. 610, 616–18 (1961) (holding unlawful the forced entry of landlord—with assistance of law enforcement—into lessee's premises).

107. *Carter*, 525 U.S. at 90, 95–97 (Scalia, J., concurring). *But see* Rakas v. Illinois, 439 U.S. 128, 141–42 (1978) (implying not all guests may able to assert Fourth Amendment protection).

108. *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting).

109. *Facebook Terms of Service*, FACEBOOK (2018), https://www.facebook.com/legal/terms [https://perma.cc/J4RN-3VE7].

110. *Id.*

111. *See Privacy Policy*, GOOGLE (Jan. 22, 2019), https://policies.google.com/privacy#infochoices [https://perma.cc/R8FW-4T6L] (allowing users to limit the information Google collects).

112. *See Facebook Data Policy*, FACEBOOK (Apr. 19, 2018), https://www.facebook.com/policy.php [https://perma.cc/E6FV-DKLP] (promising users their personal information such as name and email address will not be given to advertisers).

113. *See id.* (stating Facebook does not give out personally identifiable information unless given permission).

114. *See* Katz v. United States, 389 U.S. 347, 352–53 (1967) ("One who . . . pays the toll that permits him to place a call is surely entitled to assume that the words he utters . . . will not be broadcast to the world.").

involving the exchange of data, it is debatable if the customer should be permitted to contest a subpoena on the basis of property or quasi-property law.[115]

Electronic information in a database can be challenging to reconcile with the tangible concepts of property to which the Amendment explicitly refers. However, there are a number of approaches for extending privacy law to encompass the public's electronic footprint. Although there are many arguments for tweaking existing jurisprudence to modernize privacy rights at the national level, the top-down approach is not the only possibility. Justice Gorsuch's dissent in *Carpenter* alludes to the possibility that states will create new property rights in intangible things produced by technology.[116] The modern genesis of digital property rights in intangibles, such as email accounts and website domains, suggests that state statutes and the common law have already commenced transforming privacy law in the United States.[117]

The advancement of technology has created a sticky situation for the Court. On the one hand, it is tempting to extend the Fourth Amendment to protect one's privacy from the dangers of modern technology because so many technologies are indispensable to daily living.[118] On the other hand, extending the Fourth Amendment beyond the enumerated protections places strain on the text.[119]

The traditional search test clashed with emerging technology in the early twentieth century when telephones first came into widespread usage.[120] Many jurists recognized that law enforcement does not have to search an

115. *See* Carpenter v. United States, 138 S. Ct. 2206, 2270–72 (2018) (Gorsuch, J., dissenting) (sympathizing with the notion of states creating new property rights to solve the privacy dilemma).

116. Carpenter v. United States, 138 S. Ct. 2206, 2270–72 (2018) (Gorsuch, J., dissenting).

117. *See id.* at 2270 ("If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.").

118. Freiwald & Smith, *supra* note 96, at 225–26.

119. Griswold v. Connecticut, 381 U.S. 479, 522 (1965) (Black, J., dissenting) (rejecting the temptation to change the Constitution to keep in step with the times).

120. Olmstead v. United States, 277 U.S. 438, 464 (1928) ("The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses of offices of the defendants."), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

area physically to invade the privacy of others.[121] Police started to tap telephone lines to listen in on conversations.[122] This proved to be a beneficial tool in mitigating crime. However, it came at the expense of one's normative expectations of privacy, a concept that Justice Brandeis expounded upon around the turn of the century.[123] When the police tapped into telephone lines, there was no technical trespass, and in *Olmstead v. United States*,[124] the Court held there was no violation of the Fourth Amendment, despite the adamant protestations of Justice Brandeis.[125]

Justice Brandeis's dissent built upon his earlier writings advocating for the recognition of new rights as technology and society changed.[126] He believed jurists should not be restrained from modifying or adding to the law as needed for the common good.[127] "Legal realism,"[128] or "purposivism,"[129] a view focused on the spirit of constitutional texts, did not gain wide acceptance until the mid-twentieth century.[130] To understand the zeitgeist of the legal world at that time, scholars should note the relative slowness of incorporating the Bill of Rights under the

121. *See* Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting) ("There was no physical entry in this case. But the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment."); *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting) ("Subtler and more far reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

122. *Olmstead*, 277 U.S. at 456–57.

123. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890) (depicting the evolution of causes of action when the sanctity of one's person was encroached, either through battery, nuisance, trespass, or invasion of property rights).

124. *Olmstead*, 277 U.S. at 456–57.

125. *Id.* at 473–78 (Brandeis, J., dissenting).

126. *See* Warren & Brandeis, *supra* note 123, at 194 (declaring support for creating or extending existing rights as society changes).

127. *See Olmstead*, 277 U.S. at 476–77 (rejecting a literal construction of the Constitution when it would allegedly defeat its object).

128. *See* LAWRENCE M. FRIEDMAN, AMERICAN LAW IN THE 20TH CENTURY 271 (2002) (narrating a change in American legal philosophy heralded by legal theorist Karl Llewellyn who praised a flexible "style of reason" that considered public policy and principles).

129. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 18–19 (2012) (writing that purposivists interpreting a legal provision use the text as a starting point and adjust the level of generality to reach socially acceptable outcomes).

130. *Cf.* Griswold v. Connecticut, 381 U.S. 479, 522 (1965) (Black, J., dissenting) (criticizing the "rhapsodical strains" of the majority to make the Constitution measure up to the times).

Fourteenth Amendment and reluctance towards appearing to endorse substantive due process.[131] The 1960s saw the rapid takeoff in civil rights jurisprudence after the exclusionary rule was applied to the states in *Mapp v. Ohio*.[132] The Fourth Amendment followed this trend. The Supreme Court was no longer impressed with strict adherence to the literal letter of the law found in *Olmstead*.[133] In the year that followed, *Silverman v. United States*[134] was the last case to make significant use of the trespass test for Fourth Amendment searches.[135]

Silverman exemplified the rapid change of technology in the Cold War Era of spies and space flight when law enforcement used a "spike mike" to listen in on the activities of next-door neighbors living in an adjoining apartment.[136] The next-door neighbors permitted law enforcement to come into their living space and insert a spike mike into the wall.[137] In ruling for Silverman, the Court held that because the spike mike intruded into the section of the house owned by Silverman, law enforcement conducted a warrantless search.[138] The Court distinguished this case from earlier eavesdropping cases, but this opinion arguably sliced the trespass doctrine bread very thin. While proscribing law enforcement from intruding on private property even an inch, as long as such activity could be deemed a physical trespass, purely electronic intrusions could continue. A few years later, *Katz v. United States* overruled the previous holding in *Olmstead*—that phone tapping did not implicate the Fourth Amendment due to the absence of physical trespass.[139]

131. *See* McDonald v. City of Chicago, 561 U.S. 742, 791 (2010) (acknowledging the Second Amendment applies to the states); *see also* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 524–31 (5th ed. 2015) (recounting the arguments of various legal scholars regarding the incorporation of the Bill of Rights through the Due Process Clause of the Fourteenth Amendment).

132. Mapp v. Ohio, 367 U.S. 643, 655 (1961); *see* Miranda v. Arizona, 384 U.S. 436, 478–79 (1966) (holding individuals are entitled to be informed of their right to remain silent and obtain counsel when taken into police custody and questioned); Gideon v. Wainwright, 372 U.S. 335, 344–45 (1963) (requiring the provision of counsel to needy defendants).

133. *See* Katz v. United States, 389 U.S. 347, 352–53 (1967) (departing from the "narrow" interpretation of the Fourth Amendment in *Olmstead*).

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

135. Gerald S. Reamey, *Constitutional Shapeshifting: Giving the Fourth Amendment Substance in the Technology Driven World of Criminal Investigation*, 14 STAN. J. CIV. RTS. & CIV. LIBERTIES 201, 215–16 (2018).

136. *Silverman*, 365 U.S. at 506.

137. *Id.*

138. *Id.* at 509–10.

139. Katz v. United States, 389 U.S. 347, 352–53 (1967).

In *Katz*, the Court essentially held that the appellant had a reasonable expectation of privacy that government agents would not intercept his conversation.[140] In the majority opinion, Justice Stewart threw a wrench into the gears of Fourth Amendment jurisprudence; he stipulated that the Court's decision was based on the fact that "the Fourth Amendment protects people, rather than places."[141] Commentators have criticized him for not adequately explaining what protections people are entitled to, as it is obvious that the Fourth Amendment protects people.[142] Some jurists have described the *Katz* test as conclusory and self-indulgent.[143] By crafting a two-step test for whether one has a reasonable expectation of privacy, Justice Harlan's concurring opinion comes the closest to describing what it means to have justifiable reliance that one's privacy will not be invaded.[144]

The Court soon adopted Justice Harlan's REOP test, eschewing the traditional trespass test.[145] Justice Harlan's REOP test has two components. Whether the Fourth Amendment protects an individual's privacy depends on (1) one's subjective expectation of privacy and (2) whether the individual's expectation of privacy is one which society is prepared to accept from an objective standpoint.[146] The first part of the test is often dispensed with, leading some to remark that the REOP test has only one prong.[147]

Because it is often apparent or assumed that one subjectively believes his privacy is protected, courts often jump to the objective analysis.[148] To be of any significance, the subjective expectation must be objectively

140. *Cf. id.* at 353 (holding government wire tapping violated Katz's privacy on which Katz justifiably relied). Although Justice Harlan's concurring opinion, which created the REOP test, was not used by the majority in *Katz*, this would change within the decade. Rakas v. Illinois, 439 U.S. 128, 154 (1978).

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

142. 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE VOLUME 1: INVESTIGATION 71–72 (6th ed. 2013).

143. Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

144. *See Katz*, 389 U.S. at 360–62 (Harlan, J., concurring) (defining the reasonable expectation of privacy as "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

145. United States v. White, 401 U.S. 745, 748 (1971).

146. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

147. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015) (arguing *Katz* is "only a one-step test[,]" and "[s]ubjective expectations are irrelevant.").

148. DRESSLER & MICHAELS, *supra* note 142, at 79.

reasonable.[149] Taken literally, any declaration by the government of pervasive surveillance could eliminate one's subjective expectation of privacy.[150]

In recent years, Justice Harlan's test has, in practice, become largely a one-step objective analysis.[151] As for the objective expectation of privacy, the Supreme Court has oscillated between a couple of interpretations.[152] An expectation of privacy that "society is prepared to recognize as reasonable"[153] appears to refer to a normative expectation of privacy.[154] Justice Harlan's post *Katz* views support this interpretation of the objective prong.[155] However, the Court more often assesses whether one's expectation of privacy is empirically reasonable.[156]

An empirical view of Justice Harlan's REOP test is supported by numerous examples, including Justice Stewart's majority opinion in *Katz*.[157] Justice Stewart described a Fourth Amendment that supplies privacy protection from some forms of government intrusion, but not all.[158] He explained that, although each search case is a world of its own without a one-size-fits-all test, a person's voluntary exposure or disclosure of facts to the world renders the Fourth Amendment inapplicable insofar as the conveyed information is concerned.[159] The empirical test creates considerable tension with its key goal: flexibility in extending privacy rights.[160] Because an empirical analysis of likelihood is far removed from

149. *See id.* at 76 (recognizing "an expectation of privacy is 'reasonable' when a 'reasonable person' would not expect his privacy [to be] at serious risk").

150. *Id.* at 74.

151. Kerr, *supra* note 147, at 114.

152. *See* DRESSLER & MICHAELS, *supra* note 142, at 77 (explaining how the Court uses both the normative and empirical approaches).

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

154. DRESSLER & MICHAELS, *supra* note 142, at 77.

155. *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (supporting the notion that judges should weigh the "desirability of saddling" the public with privacy risks).

156. *See* DRESSLER & MICHAELS, *supra* note 142, at 77 (writing courts often view the fact that a privacy incursion happened as empirical evidence that the expectation of privacy was unreasonable).

157. *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

158. *Id.* at 350.

159. *Id.* at 351.

160. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 43–44 (1988) (refusing to hold search of discarded household garbage unreasonable even though the state common law created a privacy interest in garbage).

value judgments, yesterday's reasonable expectation of privacy can be overridden by technology.[161]

Some technologies allow one to scan information about the interior of the home from the outside of the home. In *Kyllo v. United States*,[162] the Supreme Court held that one has a reasonable expectation of privacy in activities within the home when technology not in general public use is employed to scan the home.[163] This holding provides a narrow exception to the general rule that information sent to the outside world is outside the scope of the Fourth Amendment. The Court in *Kyllo* declined to clarify both its meaning of common use and what would happen when technology crossed that bridge.

The empirical view of privacy led to results seemingly at odds with the goals behind *Katz*, namely an expansive third-party doctrine.[164] The Court has held that one does not have a reasonable expectation of privacy in a litany of circumstances that diminish the value of one's privacy, including financial transactions, telephone metadata, garbage left for pickup, and concealed activity in a greenhouse visible by a low-flying police helicopter.[165] This is the case even though one passes on information to third-parties with the expectation that it will be used for limited purposes.[166] Much remains unclear regarding reasonable expectations of privacy.

D. *Where Fourth Amendment Search Doctrine Stands Today*

Ultimately, the outcome under the REOP test is ethereal and mysterious. Justice Scalia and Justice Thomas have cynically remarked that the expectations of privacy that society is willing to recognize "bear an uncanny resemblance to those expectations of privacy that this Court considers

161. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451 (1989) (holding observations from a helicopter hovering 400 feet above a house did not violate any reasonable expectation of privacy).

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

163. *Id.* at 34–35. Many scholars have criticized this decision because even when this case was decided, heat scanning technology was in common use. One popular application of this technology is in heat sensing night vision goggles for hunters, which has been used for many years.

164. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976) (calling attention to the fact that deposit slips and other information that are seen by bank employees, and concluding bank records are not covered by the Fourth Amendment).

165. Carpenter v. United States, 138 S. Ct. 2206, 2266 (2018) (Gorsuch, J., dissenting).

166. *Cf.* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (suggesting a review of the current doctrine that a reasonable expectation of privacy does not extend to information voluntarily conveyed to third-parties).

reasonable."[167] The REOP test, one so flexible in nature, is the victim of its own malleability; simultaneously, the test's greatest strength is its own worst enemy.[168] Social data is not used in formulating reasonable expectations of privacy; therefore, the judge is left to his own sense of public policy, an "unruly horse"[169] that draws criticism that the Court is implementing an ad hoc doctrine reflecting its own views.[170]

From these facts, it stands to reason that, in recent years, the Court has distanced itself from the REOP test. In the early 2010s, the old trespassory test reappeared,[171] so that the Court's search jurisprudence was "said to have two heads."'[172] With *Carpenter*, the Court's jurisprudence is, arguably, now a three-headed hydra with CSLI as a distinct exception to the third-party doctrine. The Supreme Court had the opportunity to dispose of the case under the two tests above and the law governing subpoenas.[173] Instead, the Court took on a new course.

American privacy jurisprudence is at a crossroads. *Carpenter* is one in a series of inconsistent cases dating back to *Katz*. The *Katz* cases had issues of their own, but *Carpenter* is one mutation too many. Conversely, the need for meaningful privacy reform is greater than ever in a world of widespread data exchange. Challenges to privacy come from every direction, and the government is just one particular threat. Nevertheless, resolving the issue of government intrusion matters most, as one must jealously guard civil liberties from the state with every generation. A solution to the confusion surrounding privacy policy should be uniform and statutory. Other countries are ahead of the United States in this regard.[174] The courts can only resolve matters long after they have come to light. A more permanent legislative remedy is required.

---

167. Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

168. Reamey, *supra* note 135, at 232.

169. Richardson v. Mellish (1824) 130 Eng. Rep. 294, 303; 2 Bing. 229, 252.

170. *See* DRESSLER & MICHAELS, *supra* note 142, at 77–78 n.63 (observing the Supreme Court has made no serious attempt to use sociological studies in its decisions, and noting that one study shows the Court is often out-of-step with public perceptions).

171. *See Jones*, 565 U.S. at 409 (clarifying that the REOP test is a supplement to the traditional trespass analysis).

172. Reamey, *supra* note 135, at 223.

173. *See* discussion *supra* Section II.B.

174. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000) (recognizing United States privacy laws are inferior to the countries which make up the European Union).

III. WHY THE SUPREME COURT IN *CARPENTER* REACHED A LEGALLY ERRONEOUS CONCLUSION

A. *A Summary of Errors in* Carpenter

The majority in *Carpenter v. United States* makes a number of mistakes in its analysis that disserve the goals of a coherent Fourth Amendment jurisprudence,[175] the interests of law enforcement,[176] and ultimately, privacy itself.[177] A point that seems to be overlooked is that *Carpenter* calls into question whether other subpoenas for information from third parties are to be treated as searches.[178] Liberty is a defining principle in Western culture, which values individualism.[179] However, the Court's primary role is interpretation; decisions that cross the line into the Legislature's arena risk constitutional imbalance.[180]

The system of laws in the United States is largely statutory and, generally speaking, there is no expansive body of federal common law.[181] Yet, accessibility to evidence acquired through subpoenas remains critically important to law enforcement and courts of law.[182] To ensure constitutional protections, a more expansive development of Fourth Amendment jurisprudence could have provided law enforcement with a narrower means to establish probable cause to arrest

175. *See* Carpenter v. United States, 138 S. Ct. 2206, 2257 (2018) (Alito, J., dissenting) (arguing that the Court has created an independent line of case law that allows one to object to a subpoena of third-party's business records—a holding contrary to both the property-based Fourth Amendment test and the REOP test).

176. *See id.* at 2247 (criticizing an approach likely to limit the investigative powers of law enforcement and grand juries to issue a subpoena *duces tecum* without showing of probable cause).

177. *Id.* at 2261.

178. *Id.* at 2260–61 (considering the possibility that the majority's holding may generally require subpoenas for documents to be based on probable cause and the Court may have to add many interpretive nuances to clarify the majority's decision in the future).

179. *Cf.* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992) (expounding on the role of an individual's autonomous conceptualization of liberty under the Fourteenth Amendment).

180. *Cf.* Baker v. Carr, 369 U.S. 186, 339–40 (1962) (Harlan, J., dissenting) (implying the courts will only command national respect when they exercise self-restraint and discipline so as to not attempt to right every possible wrong).

181. *See, e.g.*, Erie R.R. Co. v. Tompkins, 304 U.S. 64, 78 (1938) ("There is no federal general common law. Congress has no power to declare substantive rules of common law applicable in a State whether they be local in nature or 'general,' be they commercial law or a part of the law of torts. And no clause in the Constitution purports to confer such a power upon the federal courts.").

182. *See supra* text and notes accompanying Part I.

Mr. Carpenter.[183] However, the permissible scope of probable cause is an arena where the Legislature—not the courts—should weigh the interests of security and personal privacy.[184] Courts should not intervene against policies thought to be unwise unless there is an actual legal problem.[185]

Undoubtedly, many readers will hear the originalist echo that legislatures should resolve the day-to-day challenges facing the United States.[186] It is up to the reader whether a legislative system, which has become polarized in recent years, should continue to be the focal point of lawmaking.[187] If the reader does believe in the republic, it stands to reason that courts should not spoon-feed the Legislature and create a condition of learned helplessness each time a major controversy arises.

The Supreme Court has indeed extended a helping hand to the most vulnerable in our society when it required states to furnish counsel to needy defendants[188] and commanded law enforcement to notify certain arrestees of their right to remain silent.[189] These have been positive developments in the law, but to merely focus on these effects is to miss the point: Legislatures should step up to their responsibilities as lawmakers to resolve

183. Indeed, law enforcement could have asked first for one week of CSLI data before asking for months of CSLI. *Cf.* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

184. *See* Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting) ("Answering questions like [how much privacy protection a society should have] calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts.").

185. *See* West Coast Hotel Co. v. Parrish, 300 U.S. 379, 397–99 (1937) (holding the Court should defer to the Legislature's wisdom regarding policy).

186. *See* John F. Manning, *Justice Scalia and the Idea of Judicial Restraint*, 115 MICH. L. REV. 747, 756–57 (2017) (discussing Justice Scalia's textualist approach to statutory interpretation as devoid of "elevat[ing] a statute's purpose over its enacted text"). *See generally* 2016 National Lawyers Convention, *Justice Scalia on Federalism and Separation of Powers*, 30 REGENT UNIV. L. REV. 57 (2017) (chronicalling Justice Scalia's illustrious history of citing, lecturing, and defending the separation of powers).

187. *See* Samuel A. Marcosson, *Fixing Congress*, 33 BYU J. PUB. L. 227, 236 (2019) ("[P]olarization in the House (and Senate) is less the product of systematic manipulation than it is a reflection of the wider polarization and stridency among Americans that characterizes our modern politics, and the rise of divisive (or 'wedge') issues that have increasingly fractured our politics.") (citations omitted).

188. *See* Gideon v. Wainwright, 372 U.S. 335, 344–45 (1963) (advocating representation for indigent defendants to safeguard fairness in criminal proceedings).

189. *See* Miranda v. Arizona, 384 U.S. 436, 467–68 (1966) ("At the outset, if a person in custody is to be subjected to interrogation, he must first be informed in clear and unequivocal terms that he has the right to remain silent.").

important societal questions.[190] If the American Republic is up to the task, then let it cast aside its judicial crutches. If it is incapable of protecting the freedoms for which it was founded, let a new system take its place; a system of judicial colonialism is incompatible with responsible people capable of self-rule.

The reader should bear in mind that the privacy jurisprudence before *Carpenter* was already a confusing patchwork.[191] As discussed earlier, the Court's privacy doctrine uses both the trespass test and the REOP test.[192] Chief Justice Roberts, who joined the majority opinion in *United States v. Jones*,[193] understood the value of deciding search and seizure cases on narrow grounds.[194] That is why the trespass doctrine resurfaced.[195] The REOP test shows little signs of becoming more objective and less a private value judgment of an unelected judiciary.[196] Because the REOP test proved to be a hard public policy pill for the Court to swallow, the Supreme Court cultivated the third-party doctrine to mitigate its open-ended foray into the unknown.[197] The third-party doctrine championed by crime-weary jurists alleviated much of the concern that law enforcement would be unable to carry out its duties as effectively.[198]

190. *See* U.S. CONST. art. I, § 1 ("All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives."); *cf.* Ewing v. California, 538 U.S. 11, 12 (2003) ("[T]his Court has a longstanding tradition of deferring to state legislatures in making and implementing such important policy decisions.").

191. *See* Reamey, *supra* note 135, at 204 (describing the transition from the property-based doctrine of trespass to a case-by-case adjudication approach).

192. *See, e.g.*, United States v. Jones, 565 U.S. 400, 409 (2012) ("[A]s we have discussed, the *Katz* [REOP] test has been *added to*, not *substituted for*, the common-law trespassory test.").

193. *Id.* at 401.

194. *See id.* at 411–12 (electing to use the trespass analysis when electronic monitoring involved a trespass and delaying answering the question of whether purely electronic monitoring over a long time period would violate the Fourth Amendment).

195. *Cf. id.* at 411 ("What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted.").

196. *See* Carpenter v. United States, 138 S. Ct. 2206, 2265–67 (2018) (Gorsuch, J., dissenting) (criticizing *Katz* for not clearly articulating whether the test is normative or empirical, and explaining that if it is normative, the results of *Katz* have been inconsistent, and in some cases, unbelievable given actual social norms).

197. *Cf.* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 581–85 (2009) (discussing how the third-party doctrine clarifies *Katz* jurisprudence and law enforcement).

198. *See* DRESSLER & MICHAELS, *supra* note 142, at 78 (explaining many post-*Katz* decisions reflected the same treatment they would have received under the trespass test).

Even assuming one has some expectation of privacy in the information conveyed to others, it is unclear what guidance should be used to draw the line. Intuitively, it would seem absurd to give one an expectation of privacy in the information conveyed to an undercover agent,[199] on the other hand, however, society benefits from the trust one places in a friend. Furthermore, courts would have a hard time measuring the expectation of privacy one would have in information read off a computer screen in a coffee shop.[200]

Logically, both Justice Harlan's REOP test and the third-party REOP test should have led the Court to affirm the judgment of the Sixth Circuit that the subpoena of Mr. Carpenter's CSLI was not a Fourth Amendment search.[201] This is mathematically certain when one follows third-party doctrine precedent. When one excludes third-party doctrine from the equation, the results become wildly unpredictable.

Justice Harlan's REOP test would have yielded a judgment for the government because no statute or other legal principal gave Mr. Carpenter a property interest in the CSLI.[202] Alternatively, under a more complicated analysis, Mr. Carpenter had no objectively reasonable expectation of privacy in his CSLI because that information was voluntarily conveyed to the cell company.[203] Because the empirical view of privacy has traditionally overwritten normative considerations, stare decisis should have made *Carpenter* an easy case under the REOP test's standard.[204] Information sharing is necessary in the modern world; there is no doubt that this presents problems for one's normative expectation of privacy, but this is a question of policy rather than law.

---

199. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302–03 (1966) (denying Fourth Amendment protection in conversations to undercover government agents).

200. There is ample evidence that reading off another's computer or cell phone screen violates social norms of privacy. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (emphasizing the importance of privacy with cell phones due to the sensitive data typically stored on them); WASHINGTON'S RULES OF CIVILITY & DECENT BEHAVIOR IN COMPANY AND CONVERSATION 15 (J.M. Toner ed., 1888) ("[C]ome not near the Books or Writings of Another so as to read them . . . also look not nigh when another is writing a Letter.").

201. *Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting).

202. *See id.* at 2257–59 (doubting Mr. Carpenter had a property interest in CSLI because he has no right to possession without paying the cell company a fee).

203. *Id.* at 2230 (Kennedy, J., dissenting).

204. *See* DRESSLER & MICHAELS, *supra* note 142, at 79–80 (implying that the fact that an illegal activity is witnessed is often used as a means to negate an assertion of a reasonable expectation of privacy).

The Court premised its decision that law enforcement could not obtain more than six days of CSLI without a search warrant on the novelty of the information sought.[205] The Court did not explain why six days of CSLI could be obtained without a warrant and not seven. One may only speculate on how this bright line was delineated. The Court wrote that although one would not ordinarily possess a reasonable expectation of privacy in movements knowingly exposed to others, new technology has made it possible to chronicle the near entirety of one's movements.[206] In the past, it was more costly and difficult to maintain constant surveillance of citizens.[207] In so doing, the Court sought to alleviate the near century-old concern of Justice Brandeis in *Olmstead*—that law enforcement may invade privacy using new technology if left unchecked by the judiciary.[208] Interestingly, Chief Justice Roberts applauded the foresight of Justice Brandeis in 1928, while chiding Justice Kennedy and the dissenters for failing to contemplate the "seismic shifts" in technology.[209] Legal doctrine requires that in ascertaining whether a Fourth Amendment violation has occurred, the jurist must first determine whether a search has occurred.[210] If a court decides that a search has occurred, the next question is whether the search was unreasonable.[211]

In summary, the Supreme Court erred in holding that Mr. Carpenter's Fourth Amendment rights were violated because law enforcement did not conduct a "search," as that word is understood in Fourth Amendment jurisprudence.[212] This is true for three reasons: courts do not treat

205. *See Carpenter*, 138 S. Ct. at 2220 (majority opinion) (refusing to apply the third-party doctrine "given the unique nature of cell phone location information.").

206. *See id.* at 2218 (observing that through CSLI, the government may undertake "near perfect surveillance.").

207. *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (noting that in the pre-digital age, police would not and could not monitor every movement of an individual).

208. *Carpenter*, 138 S. Ct. at 2223.

209. *Id.* at 2223. It is curious that Chief Justice Roberts dismisses Justice Kennedy's views out of hand as if he were out of touch with the realities of societal change. Justice Kennedy has provided progressive legal activists his swing vote in a number of cases concerning contentious social issues. *See, e.g.*, Russell K. Robinson, *Unequal Protection*, 68 STAN L. REV. 151, 156 (2016) (calling Justice Kennedy "the principal architect of the sexual orientation cases and the swing vote in most equality cases."). The criticism that he is out of step with the times on privacy rights seems unfair given that Justice Kennedy has never been an archconservative.

210. *Carpenter*, 138 S. Ct. at 2226 (Kennedy, J., dissenting).

211. *Cf.* Stoner v. California, 376 U.S. 483, 486 (1964) (mandating in cases of a warrantless search, the Court must examine whether a search was reasonable).

212. *See Carpenter*, 138 S. Ct. at 2226 (Kennedy, J., dissenting) (summarizing holdings of five cases interpreting the meaning of search in Fourth Amendment jurisprudence).

subpoenas for third-party business records as searches,[213] Mr. Carpenter's property was not affected,[214] and he did not have a reasonable expectation of privacy in information voluntarily exposed to a third-party.[215] The SCA requires that law enforcement seek a subpoena for electronically stored customer information from a court of competent jurisdiction.[216] The subpoena can only be issued on the showing of specific and articulable facts demonstrating reasonable grounds to believe the information is germane to a criminal investigation.[217]

B. *The Majority in* Carpenter *Erred in Applying a Heightened Standard for a Subpoena of More Than Six Days of CSLI Records, Disrupting the Longstanding Subpoena Analysis*

The Court in *Carpenter* imposed an unexpected restriction on the ability to subpoena third-party business records when it concluded a subpoena for CSLI data constituted a search.[218] It did so without further explanation and then made a logical leap to the reasonableness inquiry.[219] The Supreme Court has traditionally classified the use of a subpoena as a "constructive search."[220] Subpoenas are not as intrusive as actual searches in which a law enforcement officer enters a property and proceeds to inspect the property of another.[221] Accordingly, a subpoena *duces tecum* is held to a lower standard than probable cause.[222] A subpoena will be deemed unreasonable

213. *See id.* at 2247 (Alito, J., dissenting) (discussing how the majority ignores the difference between searches and court orders requesting production of evidence).

214. *See id.* at 2242–43 (Thomas, J., dissenting) (arguing Mr. Carpenter failed to show he had any property interest in CSLI data).

215. *Id.* at 2223–24 (Kennedy, J., dissenting).

216. 18 U.S.C. § 2703(d) (2012), *declared unconstitutional in part by Carpenter*, 138 S. Ct. at 2221 ("[T]he Government must generally obtain a warrant supported by probable cause before acquiring [CSLI].").

217. *Id.*

218. *Carpenter*, 138 S. Ct. at 2220 (majority opinion).

219. *Cf. id.* at 2235 (Kennedy, J., dissenting) (disagreeing with the Court's holding that an unreasonable search occurred without first remanding the case to determine if the search was unreasonable).

220. *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 201–04 (1946) (detailing the confusion between actual searches and constructive searches).

221. *See Carpenter*, 138 S. Ct. at 2228 (Alito, J., dissenting) (explaining that a warrant "allows the Government to enter and seize and make examination itself" whereas a subpoena "requires the person to whom it is directed to make the disclosure"); *cf.* Riley v. California, 573 U.S. 373, 403 (2014) (identifying the primary force behind the Fourth Amendment as the practice of British soldiers "rummag[ing]" through homes by means of general warrants).

222. *Oklahoma Press Pub. Co.*, 327 U.S. at 208.

under the Fourth Amendment if the government abuses its power with an indefinite request for production.[223]

When an individual receives a subpoena, the respondent collects the necessary documents or things to be produced.[224] There is no invasion of privacy apart from the production of the items demanded in the subpoena,[225] and because the individual has an opportunity to object to the subpoena as unduly burdensome, there is some recourse.[226] In a search, the law enforcement officer is entitled to use reasonable force to fulfill his investigatory role,[227] and the one being searched only has a cause of action after the fact if the search was unreasonable.[228]

Although an individual whose cell site location information is sought will not be pleased by law enforcement knowing their whereabouts, CSLI is the property of the cell company under existing law. The Fourth Amendment protects citizens in "*their* persons, houses, papers, and effects"[229]; any privacy rights protected by the Fourth Amendment are necessarily linked to property rights, even if the REOP test does not require technical trespass.[230] Because a cell company creates the records of CSLI in the course of connecting a customer's phone to the network as well as in billing for roaming charges, this constitutes a cell company's proprietary information.[231]

223. *See id.* ("[T]he Fourth [Amendment] . . . guards against abuse only by way of too much indefiniteness . . . . The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.").

224. *Carpenter*, 138 S. Ct. at 2228 (Alito, J., dissenting).

225. *See id.* (explaining that the option to object to the subpoena "mitigates the intrusion").

226. *Id.*

227. *See* United States v. Ramirez, 523 U.S. 65, 71–72 (1998) (concluding police officers acted reasonably by breaking windows during a search to prevent occupants from grabbing firearms in the garage); Brown v. Battle Creek Police Dep't, 844 F.3d 556, 572 (6th Cir. 2016) (concluding police officers acted reasonably in shooting two dogs during a search); *cf.* Donovan v. Lone Steer, Inc., 464 U.S. 408, 414 (1984) (explaining how searches involve unconsented entry into areas forbidden to the general public).

228. *Cf. Oklahoma Press Pub. Co.*, 327 U.S. at 195 (implying a subpoena gives the recipient the opportunity to contest a request when he suffers injury unlike an actual search).

229. U.S. CONST. amend. IV (emphasis added).

230. *Carpenter*, 138 S. Ct. at 2227–28 (Kennedy, J., dissenting) (claiming that privacy rights are necessarily rooted to "commonsense principle that the absence of property law analogues can be dispositive of privacy expectations"); Rakas v. Illinois, 439 U.S. 128, 143 (1978) ("[I]f police officers had not been guilty of a common law trespass they were not prohibited by the Fourth Amendment from eavesdropping . . . .").

231. *Carpenter*, 138 S. Ct. at 2229–30 (Kennedy, J., dissenting).

Once the CSLI information is anonymized, the cell company will often sell this information.[232] Even assuming that the subpoena constituted a search, Mr. Carpenter should not have been entitled to raise an objection because he could not have raised a cause of action for which the law could offer relief.[233] Admittedly, one intuitively believes CSLI is generally kept private from the general public, and this implicit understanding is reflected in the fact that cellular providers anonymize user data prior to selling it. Nevertheless, the fact that the law has not caught up with society is not sufficient cause for the court system to intervene. Absent a statutory or constitutional change, subpoenas are proper for acquiring evidence, whether or not the proponent has demonstrated probable cause.[234]

Subpoenas have been used in the common law for many years.[235] History reveals the propriety of court orders for production pursuant to an investigation.[236] The Framers of the Constitution were aware of the subpoena *duces tecum* during the drafting of the Fourth Amendment.[237] If the Framers had intended to attach a standard of probable cause to subpoenas, they most likely would have included that provision. The founders were indeed concerned about the "privacies of life,"[238] but the overarching concern was the destruction and abuse of property rights.[239] It is hornbook law that the power to exclude is the foremost aspect of property.[240] Requiring a search warrant for the most intrusive means of

232. *Id.* at 2212 (majority opinion).

233. *See* FED. R. CIV. P. 12(b)(6) (permitting a motion to dismiss for failing to state a claim on which relief may be granted); Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (refusing to accept that one has a reasonable expectation of privacy in telephone numbers dialed and thus voluntarily provided to the telephone company); United States v. Miller, 425 U.S. 435, 442–43 (1976) (declining to extend the Fourth Amendment to protect the privacy of bank client's financial records).

234. *Cf.* Hale v. Henkel, 201 U.S. 43, 73, 76 (1906) (generally exempting subpoenas from the intense scrutiny of the Fourth Amendment apart from a reasonableness analysis on the grounds that justice would otherwise be impeded).

235. *E.g.*, Rex v. Dixon [1765] 97 Eng. Rep. 1047; 3 Burr. 1685.

236. *See* Blair v. United States, 250 U.S. 273, 280 (1919) (recognizing the inquisitorial power of grand juries to compel production of evidence and the testimony of witnesses).

237. *See Carpenter*, 138 S. Ct. at 2249–50 (Alito, J., dissenting) (concluding the founders supported the concept of the grand jury because they were aware of its powers, including the subpoena of evidence).

238. Boyd v. United States, 116 U.S. 616, 630 (1886).

239. *See Carpenter*, 138 S. Ct. at 2240 (Thomas, J., dissenting) (declaring property the "organizing constitutional idea of the founding era").

240. *See* Dickman v. Comm'r, 465 U.S. 330, 336 (1984) ("Property is composed of constituent elements and of these elements the right to *use* the physical thing to the exclusion of others is the

acquiring evidence struck a balance between property rights and the execution of the law.

Property rights, like all other rights, are not unlimited.[241] The Supreme Court has expounded "the ancient proposition of law" that "the public has a right to every man's evidence."[242] Law enforcement often requires the power to issue a subpoena to build enough evidence to establish probable cause to arrest dangerous criminals, including murderers and rapists.[243] In the case of Mr. Carpenter, a man who conducted a series of six robberies across multiple states,[244] CSLI data was well-suited to building circumstantial evidence implicating him in the robberies.[245] Additional data regarding his whereabouts over a longer time period would also establish whether he typically visited these areas.[246] If Mr. Carpenter had regularly visited these areas in the past, such evidence might prove exculpatory.[247]

A subpoena *duces tecum* is not only useful to law enforcement, but to grand juries as well.[248] Their impact would be significantly reduced if law enforcement required probable cause every time they sought to produce information.[249] The only case to hold that probable cause is required for a subpoena was *Boyd*, and courts quickly retreated from that view.[250] In *Carpenter*, the Court appeared to resurrect this view.[251] Clear precedent in *Smith v. Maryland*[252] and *United States v. Miller*[253] dictates otherwise.[254]

---

most essential and beneficial." (quoting Passailaigue v. United States, 224 F. Supp. 682, 686 (M.D. Ga. 1963))).

241. *Cf.* District of Columbia v. Heller, 554 U.S. 570, 635 (2008) (holding the Second Amendment, like most rights, is not unlimited); United States v. Williams, 553 U.S. 285, 288 (2008) (restating that freedom of speech does not protect obscenity).

242. United States v. Nixon, 418 U.S. 683, 709 (1974).

243. *Carpenter*, 138 S. Ct. at 2233–34 (Kennedy, J., dissenting).

244. *Id.* at 2212 (majority opinion).

245. *Id.* at 2226 (Kennedy, J., dissenting).

246. *Id.*

247. *Cf. id.* (observing that if Mr. Carpenter had visited any less regularly, it became more likely that he had participated in the robbery).

248. United States v. Calandra, 414 U.S. 338, 343 (1974).

249. *Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting) (listing the adverse consequences to investigations of terrorism, political corruption, and white-collar crimes if subpoenas required probable cause).

250. *Id.* at 2253.

251. *Id.* at 2255.

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

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

254. *Carpenter*, 138 S. Ct. at 2228 (Kennedy, J., dissenting).

In *Smith* and *Miller*, telephone call metadata and bank records were sought via subpoena, and the Supreme Court held there was no search in either case.[255] The Court in *Carpenter* distinguished these analogous cases by suggesting that CSLI on a person's whereabouts is a different category of data altogether.[256] However, information relating to who a person calls, and where and to whom a person exchanges money, is arguably more intrusive to privacy.[257] Such information can reveal associations, as well as a person's private beliefs and interests.[258]

C. *The Supreme Court's Holding in* Carpenter *Cannot Be Justified Under Fourth Amendment Trespass Doctrine Because Mr. Carpenter Had No Property Interest in His CSLI*

Another hurdle for Mr. Carpenter was that he could not prove that he had a property interest in his CSLI.[259] In fairness, it is sensitive information, but as a matter of law, he nevertheless lacks any kind of property interest.[260] Mr. Carpenter argued that he had a right to his CSLI under the SCA.[261] While Mr. Carpenter may request to see his CSLI data, he is not entitled to possession.[262] The cell company is entitled to payment to produce the information.[263] This is inconsistent with customer data ownership if the customer must pay to take possession of his alleged property.[264]

Because Mr. Carpenter did not have any quantum of data ownership, he was not entitled to contest the subpoena, nor was he able to succeed under the trespass theory.[265] However, under a trespass analysis, one must consider more than the fact that the SCA is inconsistent with the ownership of CSLI data. In particular, one must look at whether CSLI could be

255. *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 444.

256. *Carpenter*, 138 S. Ct. at 2232 (Kennedy, J., dissenting).

257. *See id.* (illustrating the vast amount of information the Government gathers through the use of cell-site records).

258. *Id.*

259. *Id.*

260. *Id.* at 2257–59 (Alito, J., dissenting).

261. *Id.*

262. *Id.* at 2257.

263. *Id.* at 2258.

264. *Id.*

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

considered one's "papers" or "effects."[266] The trespass doctrine, after all, encompasses an enumerated set of protected things.[267]

It is difficult to argue that CSLI is one of Mr. Carpenter's papers. Even though one can see analogues to papers in many digital aspects of life, just as one can see analogues to free speech in physical acts[268] and t-shirt messages,[269] there is nothing comparable to papers in CSLI. Papers appear to refer to compositions of words or other creative means of expression. This meaning is reinforced by Dr. Samuel Johnson's dictionary, which defines paper as the "substance on which men write and print."[270] CSLI itself cannot be reconciled with the eighteenth-century definition of papers, as it is not a medium for composing thoughts like physical paper. A unit of CSLI is a relative geographic measuring stick indicating one was within a physical area.[271] CSLI is most likely an effect under the Fourth Amendment, as effects capture nearly all chattels.[272] At first glance, it appears to be a stretch to include bits of data, given that the contents themselves are intangible. However, courts should not be rigid about extending the idea of property, even if it is in electronic form.

If Mr. Carpenter had some creative input in the making of CSLI, he might have had a claim that it was one of his papers.[273] What is not clear is: what property interest, if any, a person has in their own physical movements. The Supreme Court has previously stated that one does not have an expectation of privacy in movements made and conveyed in public to anyone watching,[274] but this alone does not answer whether a person has a property interest in the totality of one's physical movements. Perhaps the principles

266. *See id.* at 2272 (Gorsuch, J., dissenting) (expressing belief CSLI might be papers and effects but determining issue was not adequately developed in lower court).

267. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects . . . .").

268. *See* Texas v. Johnson, 491 U.S. 397, 420 (1989) (holding flag burning is considered an exercise of free speech).

269. *See* Cohen v. California, 403 U.S. 15, 26 (1971) (explaining how wearing a t-shirt is considered exercising free speech).

270. *Paper*, 2 A DICTIONARY OF THE ENGLISH LANGUAGE (1967).

271. *Carpenter*, 138 S. Ct. at 2232 (Kennedy, J., dissenting).

272. Brady, *supra* note 94, at 948–51 (assuming from the relevant case law that "effects" encompass all personal property).

273. *See* Ruckelhaus v. Monsanto Co., 467 U.S. 986, 1020 (1984) (recognizing a property right in trade secrets); JESSE DUKEMINIER ET AL., PROPERTY 64 (Vicki Been et al. eds., 8th ed. 2014) (explaining how ideas can become property if used to compose an imaginative work).

274. *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding an individual had "no reasonable expectation of privacy" while driving his automobile in public).

of the common law support a right to at least some ownership. Property is, after all, a bundle of rights. One may have a differing quantum of property ownership such as a fee simple absolute, a life estate, or a term of years, and the government is bound to respect those property rights.[275]

The closest analogues the author has found to a property claim in one's physical movements are claims for damages based on property ownership in one's likeness or personality,[276] one's biological cells,[277] and one's ideas.[278] From a theoretical standpoint, it would appear that a claim of interest in one's movements falls on a tangibility spectrum ranging from one's ideas on one end to one's cells on the other. Mere ideas are not considered property,[279] although they can become property if used to compose an imaginative work or create a new invention.[280] The statutes regulating patent and copyright law provide the legal backbone for property rights in science and literature.[281] Even this kind of intellectual property is a limited social construct to promote innovation, rather than a physical reality such as a man-made structure on a plot of land.[282]

There is an ongoing debate as to whether cells are property,[283] and one only has a claim to one's personality or likeness if it is appropriated for profit, such as advertising in a person's name.[284] On the other hand, videotaping someone in public in itself would not impose on anyone's

275. *See* Minnesota v. Carter, 525 U.S. 83, 95–96 (1998) (noting one is not required to hold property in fee simple to be protected by the Fourth Amendment).

276. *See* White v. Samsung Elec. Am., Inc., 971 F.2d 1395, 1397 (9th Cir. 1992) (holding a person's right of publicity may be violated not only by use of the person's "name or likeness," but also by impersonation).

277. *See* Moore v. Regents of Univ. of Cal., 793 P.2d 479, 493 (Cal. 1990) (holding that while excised cells may be property in certain situations, their use for medical research does not support a conversion cause of action).

278. *See* Diamond v. Chakrabarty, 447 U.S. 303, 309–10 (1980) (holding manmade bacterium was patentable because it was the "product of human ingenuity").

279. For example, an invention must be patentable by fitting enumerated criteria. 35 U.S.C. § 101 (2012).

280. *See* DUKEMINIER ET AL., *supra* note 273, at 76–77 (explaining the value of intellectual property protections and describing their requirements).

281. *See id.* (describing the purpose and requirements of obtaining a copyright or patent on one's work).

282. *Id.*

283. *See id.* at 101–03 (discussing public policy considerations implicated if cells are recognized as property and the injustice that may result when they are not recognized as such).

284. *See* White v. Samsung Elec. Am., Inc., 971 F.2d 1395, 1397 (9th Cir. 1992) (reflecting on the origin of common law publicity rights, namely the interest in exploiting one's image for commercial gain).

property interest.[285] Although the plurality of the *Carpenter* Court addressing the property rights issue did not proceed to address all of the property right possibilities exhaustively, it appears almost ludicrous to suggest a property right in one's recorded movements.

Another factor to consider is whether the terms and conditions supported Mr. Carpenter's allegation that he had a property interest in CSLI. There is no evidence that he had a contractual right to any of this through the cell phone company, even though the market provides many examples of the recognition of property rights in user data.[286] Because Mr. Carpenter does not have a property interest in CSLI by statute, at common law, or by contract, it is time to move on to the final test for privacy rights under the Fourth Amendment. Over the years, the Supreme Court has established that property ownership is not the only factor considered in deciding whether one has a Fourth Amendment claim.[287]

D. *The Majority in* Carpenter *Erred in Holding One Has a Reasonable Expectation of Privacy in CSLI Because One Voluntarily Conveys This Information to the Cell Phone Company*

What a person attempts to preserve as private may be protected by the Fourth Amendment under the REOP test.[288] The first step in the analysis is whether Mr. Carpenter had a subjective expectation of privacy.[289] Courts have often skipped over this step to the objective test because the subjective expectation of privacy is subordinate to the objective test.[290] As harsh as the results of the law may indicate, Mr. Carpenter could not have had a reasonable subjective expectation of privacy. By carrying the cell phone while it was on, Mr. Carpenter pinged any nearby cell towers as he went about his legitimate and criminal business.[291]

Mr. Carpenter reasonably should have known that the cell phone, while it was on, had the capacity to make a call or receive a call whenever it was

285. *Cf.* United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

286. Cook, *supra* note 6 (recognizing customers' privacy interest in their data).

287. Katz v. United States, 389 U.S. 347, 352–53 (1967).

288. *Id.* at 351–52.

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

290. DRESSLER & MICHAELS, *supra* note 142, at 79.

291. *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) ("A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call.").

on. To do this, the cell phone had to consistently connect to nearby towers. Nearly everyone who uses a cell phone understands this principle. When a person enters a region with few cell towers, the reception decreases. The quantity of cell reception bars registers to the user on the screen. This affects the ability to make a call, the quality of a conversation, the ability to receive calls or messages, and the capacity to surf the Internet.

Because Mr. Carpenter did not have a valid subjective expectation of privacy, he cannot succeed on a theory that he is entitled to Fourth Amendment protection under the REOP test. However, assuming for the sake of argument, as past courts have done, that Mr. Carpenter did have a subjective expectation of privacy, he still fails to pass the objective prong of the test. There was originally a split of opinion as to whether the objective prong of the test, which is based on expectations "society is prepared to recognize as 'reasonable,'"[292] calls for a normative or empirical analysis.[293]

Although the goal of the *Katz* test is to preserve normative expectations of privacy, the Supreme Court has weighed the extent to which a person exposes himself more heavily against the privacy proponent.[294] In *Katz*, the type of exposure factored into the case's outcome.[295] *Katz* involved a man stepping into a phone booth.[296] He could be seen through the transparent glass, but he sought privacy in his conversation; he reasonably anticipated being watched, and that aspect of privacy did not matter in the analysis.[297] Thus, the objective prong of the test has been interpreted in more recent years as much more empirical than normative.[298] In other words, what a person knowingly exposes to the general public is never protected by the REOP test.[299]

292. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

293. Justice Gorsuch believes this matter is still undecided. Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting).

294. In other words, the fact that an individual is observed is often deemed evidence that an expectation of privacy was objectively unreasonable. DRESSLER & MICHAELS, *supra* note 142, at 77.

295. *Katz*, 389 U.S. at 352 (majority opinion).

296. *Id.* at 348.

297. *Id.* at 352.

298. DRESSLER & MICHAELS, *supra* note 142, at 77.

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

For example, a person generally has no reasonable expectation of privacy in his physical movements.[300] *United States v. Knotts*[301] is clear on this point and should have been applied in *Carpenter*. In *Knotts*, police placed a "beeper" tracking device in a drum of chloroform, which was subsequently purchased and loaded into Mr. Knotts's automobile.[302] Police tracked the automobile and eventually found probable cause to arrest the man for crafting illegal methamphetamine.[303] Because his physical movements were voluntarily conveyed to anyone who watched, he did not have a reasonable expectation of privacy.[304]

The fact that the empirically objective inquiry trumps the normative component is especially visible in *California v. Greenwood*.[305] In that case, law enforcement sifted through the contents of a person's garbage.[306] The dissent noted how most people would be outraged to see someone looking through their garbage to uncover information about them.[307] Indeed, garbage could reveal information about a person such as alcohol consumption, or whether an individual is affiliated with particular charities or organizations.

The dissent in *Greenwood* recited the distress that renowned statesman, Henry Kissinger, underwent when the press published a report based on private notes obtained from their garbage.[308] At the time, the State of California even had a law stating one has an expectation of privacy in garbage left for sanitation workers to collect.[309] Despite all clues as to society's normative expectations, the Court held there was no reasonable expectation of privacy in garbage placed at the street corner for collection.[310]

300. *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding one has no reasonable expectation of privacy in movements on a public roadway).

301. *Id.* at 276.

302. *Id.* at 278.

303. *Id.* at 278–79.

304. *Id.* at 281–82.

305. California v. Greenwood, 486 U.S. 35 (1988).

306. *Id.* at 37–38.

307. *Id.* at 51–52 (Brennan, J., dissenting).

308. *Id.*

309. *Id.* at 43 (majority opinion).

310. *Id.* at 41.

Likewise, people do not have a reasonable expectation in activities another can view from a public vantage point.[311] In *California v. Ciraolo*,[312] a marijuana farmer "hid" his marijuana plants in his backyard.[313] The plants were not viewable from the ground level due to fencing, which obscured the view.[314] An anonymous source notified police, who proceeded to take an aircraft over the lot to verify the accuracy of the informant's statements.[315]

The police observed marijuana plants from above and arrested the grower.[316] The grower argued he had a reasonable expectation of privacy because it was unlikely that most casual observers would have noticed the marijuana plants.[317] Nevertheless, the low probability of being detected did not matter to the Court, as the plants were still visible from a public vantage point.[318] Because one does not have a reasonable expectation of privacy to information knowingly conveyed to the public, the third-party doctrine applied.[319]

The third-party doctrine is best illustrated by Benjamin Franklin's proverb: "Three men can keep a secret if two of them are dead."[320] One does not have an expectation of privacy in a conversation with one who is secretly a government agent.[321] The criminal must fall on the sword of the false friend.[322]

Likewise, as the background section pointed out, numerous exchanges of information from daily life fall under the third-party doctrine. Whenever individuals drive to the store to buy groceries, their transactions generate a

311. *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) (refusing to insist police avert their eyes from information derived from public vantage point).

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

313. *Id.* at 209–10.

314. *Id.* at 211.

315. *Id.* at 209–11.

316. *Id.* at 209–10.

317. *See id.* at 211 (noting respondent's argument that he did all he could to shield his activities from view).

318. *Id.* at 213.

319. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding the Fourth Amendment does not protect what is knowingly exposed to the public even in private areas).

320. RHETORIC AND THE DISCOURSES OF POWER IN COURT CULTURE: CHINA, EUROPE, AND JAPAN 178 (David R. Knechtges & Eugene Vance eds. 2005).

321. *See* United States v. White, 401 U.S. 745, 752 (1971) (stating the law provides no protection to the criminal whose accomplice is a government agent).

322. *See id.* (stating a defendant who distrusts their companions should discontinue their association or risk the consequences).

record of some kind. If they pay in cash, they leave less of a footprint than if they pay with a credit card or a check. Unfortunately, the technological footprint a person leaves is the price of living in the modern era, until legislation can catch up with the times.

IV. THE SOLUTION TO AMERICAN PRIVACY RIGHTS IS A COMBINATION OF CONSTITUTIONAL AND STATUTORY PROTECTIONS

The Fourth Amendment continues to provide protection from numerous kinds of intrusion that the Framers envisioned, but existing doctrines provide little help for people in Mr. Carpenter's position. In Mr. Carpenter's case, the use of a cell phone automatically transmitted CSLI to the cell phone company.[323] Realistically, in a world of adhesion contracts, the average consumer will rarely set forth the terms of service with respect to data. These contracts are "take it or leave it" in nature, and, more importantly, certain data cannot be deleted for business or regulatory purposes.

The present incompatibility of technology and personal privacy does not make the third-party doctrine any less applicable. However, the reader must understand that the Fourth Amendment cannot resolve certain kinds of privacy intrusion. There are so many more ways that privacy can be intruded upon in the modern age than existed at the time the Constitution was written.

In *Carpenter*, the Supreme Court held that cell site data is qualitatively different than any other form of information, but again, the Court struggles to show that purchases or dialed phone numbers present any fewer privacy concerns.[324] The Court's decision inconsistently applies its precedents and incorrectly assumes that the writers of the Constitution intended the Fourth Amendment as a patch for all future privacy intrusions. The Court thinly veils its application of natural law theory.

Concern from the public should not have led to a judgment for Mr. Carpenter under subpoena law, the trespass doctrine, or the REOP test because the Court exists to interpret and apply the law dispassionately. Substantive outcomes are not the Court's area of expertise, and to ensure the structural integrity of separation of powers, the Court should decline to make future *Carpenter* exceptions. This conundrum begs the question of how the law should be changed. Indeed, it is concerning that 127 days of

323. Carpenter v. United States, 138 S. Ct. 2206, 2212, 2220 (2018).

324. *Id.* at 2232 (Kennedy, J., dissenting).

Mr. Carpenter's data could become known by the authorities. At the same time, the Fourth Amendment impedes certain types of unreasonable intrusion, but not others.[325]

Danger follows the Court's well-meaning attempts to protect the privacy of Americans. What the courts may give the courts may also take away. In times of great controversy, the rights of Americans are at the greatest risk. One recalls the attempts at mass surveillance following the 9/11 terrorist attacks.[326] The meaning of the Fourth Amendment should not be amenable to either supplementation or erosion.

Carpenter has the real potential to confuse the judicial system and law enforcement as it is unclear whether other forms of third-party owned electronic data will be singled out for a warrant requirement.[327] There is no guidance on what other information fits within an exception to the third-party doctrine.[328] Likewise, it is a mystery why the Court creates an exception to its new warrant requirement for less than seven days of CSLI as opposed to a different metric.[329] This case may be a unicorn among cases, but the existence of one of these cryptic exceptions raises the possibility that more will come to light. Even though the Court stopped short of invalidating its third-party case law in *Miller* and *Smith*,[330] these cases could be up next to be dismembered.

Whether the dismemberment of the case law in *Smith* and *Miller* is good or bad, there are reasonable arguments to be made for allowing third-party information to be subpoenaed or for strictly curbing the surveillance apparatus. The author believes in halting the surveillance state, but the solution eludes the wisest. Americans see the writing on the wall regarding privacy and what will happen if society fails to answer the fundamental question of privacy rights. One need only look to Europe to see a free society turned Orwellian. In Britain, there are cameras on every street corner, and members of parliament advocate punishing those who view

325. *See* Hester v. United States, 265 U.S. 57, 58 (1924) (concluding law enforcement would not run afoul of the Fourth Amendment in an open field even if they were trespassing); United States v. Beene, 818 F.3d 157, 162 (5th Cir. 2016) (elaborating that a driveway is not part of a house's curtilage for Fourth Amendment purposes).

326. Peralta, *supra* note 8.

327. *Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting).

328. *Id.* at 2232.

329. *Id.* at 2234.

330. *Id.* at 2216–17 (majority opinion).

politically controversial videos online.[331] Closer to home, the CIA spied on members of Congress and lied about it.[332] The IRS has selectively targeted conservative and far-left organizations for disparate treatment in the past several years.[333]

An out-of-control surveillance state is not a new problem in the United States. The Church Committee in the 1970s uncovered misconduct by intelligence agencies during the Nixon presidency and earlier.[334] As early as the 1930s, J. Edgar Hoover, the first director of the Federal Bureau of Investigation, abused his power to spy on presidents and those with viewpoints disagreeable to him.[335]

All of these factors show the importance of taking action. The question remains as to what action should be taken. Some have proposed the libertarian view of letting the free market provide solutions to privacy.[336] The issue with the libertarian view is that one is at the mercy of the market with no means of enforcing one's privacy rights at law. Modern libertarianism generally fails to account for the problem of "bad neighbors" in the marketplace who are so powerful that they are insulated from attempts at individual consumers ostracizing them. Privacy needs a backup plan—just as the Uniform Commercial Code is a fail-safe for when private

331. *See* Alan Travis, *Amber Rudd: Viewers of Online Terrorist Material Face 15 Years in Jail*, THE GUARDIAN, (Oct. 2, 2017, 7:57 PM), https://www.theguardian.com/uk-news/2017/oct/03/amber-rudd-viewers-of-online-terrorist-material-face-15-years-in-jail [https://perma.cc/6Y6R-RQPY] (describing British Home Secretary Amber Rudd's plan to criminalize viewing far-right videos online among other materials deemed to be extremist); David Barrett, *One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey*, THE TELEGRAPH (Jul. 10, 2013, 6:30 PM), https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html [https://perma.cc/A2YB-VT2L] (discussing the ubiquitous closed-circuit television cameras in Britain).

332. *See* Fenn, *supra* note 7 (referencing legal spying committed by the CIA).

333. *See* Editorial, *The IRS Targets Conservatives*, WALL ST. J., May 11, 2013, at A14 ("Internal Revenue Service official disclosed for the first time . . . that the agency that wields the taxing power of the federal government has targeted conservative groups for special scrutiny during the 2012 election season.").

334. *See* S. REP. NO. 94–755, at 12–18 (Comm. Print 1976) (referencing government agency misconduct).

335. *See id.* at 38–51 (exposing the FBI's domestic surveillance and harassment of advocacy groups and civil rights leaders, media manipulation, threatening of controversial professors and writers, and reading American mail supplied by the CIA); Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233, 244 (2017) (detailing Director Hoover's wiretaps on "members of Congress, union officials, political activists, and civil rights and religious leaders.").

336. *See* GRAY, *supra* note 12, at 106 (demonstrating how consumer demand for products offering security pushes new technology advancements).

parties to a commercial agreement fail to reach a settlement outside of the courts. In some cases, it may indeed be in a company's best interests to protect consumer data privacy by resisting government acquisition of data.[337] In other situations, a company may bend under the pressure of a major lawsuit.[338]

In other countries, the banning or regulating of message encryption has caused many email encryption companies to go out of business, leaving their consumers without any privacy.[339] The market-based solution may work in many cases, but it is still subject to being overridden by the state, and the law should provide some kind of safety net for when the free market fails to provide a solution.

Another proposed solution may be to limit the implementation of new investigation or surveillance techniques without express statutory authorization.[340] This is the law currently used in the European Union. This too seems to miss the mark of a privacy solution. A blanket ban may provide for additional privacy until the next legislative session—a temporary delay at best—but in the interim, it may tie down law enforcement excessively.

Yet another view is to judicially implement a normative expectation of privacy upon law enforcement and leave *Katz* largely untouched.[341] Such a viewpoint is similar in many ways to the approach in *Carpenter*, except that the focus on technology is less relevant to the inquiry.[342] Instead, courts would consider a number of factors, including social norms, the intent of law enforcement action, and whether a technique is particularly invasive or intrusive to the principles behind the Fourth Amendment.[343] This approach will ultimately fail to preserve normative expectations of privacy because these norms can fluctuate in multiple directions. It can also evolve

337. *See id.* at 107 (highlighting Apple's successful contest of FBI's demand that the company write a program to circumvent security and encryption software on iPhones).

338. *See id.* ("Google, Yahoo, and other major search engines receive thousands of demands each year for user information . . . . Telephone service providers respond to thousands of demands each year from law enforcement agencies for information about users' calls.").

339. *See id.* at 108 (discussing the rise and fall of encrypted email services such as Lavabit and Silent Circle).

340. Freiwald & Smith, *supra* note 96, at 235.

341. Reamey, *supra* note 135, at 237–38 (believing a more "holistic view of reasonable expectation of privacy" would be more "faithful" to *Katz*).

342. *See id.* at 244 (discussing irrelevancy of "old" versus "new" technology).

343. *See id.* (outlining relevancy of societies expectations, investigative intent, and intrusiveness of search).

in such a way that privacy guarantees shrink below what the Framers of the Constitution intended. The law would be placed at the mercy of social scientists or the jurist's own expectation of privacy. The physical sciences are based on experimental data and patterns that can be recreated multiple times, yet entire theories are subject to constant revision; the social science fields have never enjoyed even that much mathematical certainty.

The problem at hand may also be addressed provincially by each state in the form of new property laws.[344] States could create property interests in electronic information.[345] However, there still may be issues where based only on locally binding law, companies have the sole property right to customer information.

The Supreme Court could impose quasi-property standards on transactions. For example, in *Katz*, one could interpret the Court's decision as recognizing a quasi-property principle in a phone call because the individual paid for the use of the phone, as well as the phone booth, and shut the door.[346] One could argue that a Fourth Amendment quasi-property interest was created through an implied understanding that the phone company would honor the consumer's privacy. By paying for the service, *Katz* stepped into the shoes of the phone company that owned the phone booth. When government agents trespassed on the company's phone line by attaching a listening device, the interlocutor stepped into the shoes of the company and had a Fourth Amendment claim. This quasi-property theory greatly stretches the meaning of the Fourth Amendment and would enlarge the power of the judiciary.

Lastly, some legal scholars believe in keeping the third-party doctrine as it is and allowing the common law and statutes to provide protections for individuals.[347] This theory relies upon a mosaic of common law privileges such as attorney-client, priest-penitent, etc., as well as statutes to create a risk insurance plan for privacy.[348] This ad hoc approach has some benefits in that the third-party doctrine aids law enforcement in the prosecution of crime, and the combination of common law and statutes impose certain

344. *See* Carpenter v. United States, 138 S. Ct. 2206, 2270 (2018) (Gorsuch, J., dissenting) ("If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking . . . .").

345. *Id.*

346. Katz v. United States, 389 U.S. 347, 352 (1967).

347. *See* Kerr, *supra* note 197, at 565–66 (encouraging "nonconstitutional legal principles" to deter police harassment of third parties for information).

348. *Id.* at 597–99.

limits.[349] Its key defect is that the third-party doctrine will swallow up whatever privacy is not explicitly protected by law, and even the temporary privacy one has can be taken away by a later statute. Meanwhile, judges are pressed into making often inconsistent value judgments about privacy to fill in statutory gaps between the public's privacy expectations and what is not explicitly forbidden. One does not have the assurances and permanence of a constitutional provision addressing matters technically outside of the Fourth Amendment.

What is clear is that the Supreme Court's value judgments on public policy escalate tensions and polarize the political sphere, since their precedents establish the forbidden fruit of public sentiment. The anxiety and doubt of the public concerning the judiciary has reached a fever pitch. When Justice Scalia passed away, there was panic among conservatives that President Obama would redefine the country by shifting the philosophical balance on the Supreme Court. Conversely, when Justice Kennedy retired, liberals were calling the occasion a national crisis. A republic is largely built upon a foundation of faith in its institutions. This should be restored by reining in the exercise of judicial power. There is only so much that jurists in robes can do under Article III of the Constitution.[350] The republic would be better served by resolving controversies such as privacy through the legislative branch.

The proper approach to protecting and preserving privacy for the American people is a combination of constitutional and statutory change. It is hard enough to get an act of Congress passed, let alone a constitutional amendment.[351] However, the hard road must be taken to test whether this republic can function. If the judiciary takes a backseat, the demand for privacy will accelerate the action of legislative bodies.

One factor to consider in the proposed course of action is that many statutes are already in place. A patchwork of statutes is not a bad answer to complicated societal issues. Congress has passed acts regulating stored communications and the use of pin registers.[352] No solution to the privacy dilemma will be perfect. It need only provide reasonable safeguards against government tyranny through oppressive surveillance. For example, a law or

349. *Id.* at 567–70, 596–600.

350. *See* U.S. CONST. art. III (limiting judicial power to only those circumstances specifically mentioned in Article III).

351. STORY, *supra* note 69, at xxix–xxx.

352. 18 U.S.C. § 2703 (2012).

constitutional amendment could prevent the government from establishing a nationwide system of closed-circuit television cameras on every street corner, similar to the United Kingdom. The government could still install security cameras on its own property, but it could not force private individuals to install cameras on the outside of buildings or otherwise cooperate in a surveillance scheme.

In the case of Mr. Carpenter, the SCA provided some safeguards by requiring law enforcement to produce specific and articulable facts showing the information sought would be relevant to a criminal investigation before securing a subpoena to access Mr. Carpenter's CSLI.[353] Mr. Carpenter's privacy rights could have been better protected by requiring police to not only establish probable cause, but also require the CSLI request be limited to a particular day in which the suspect is alleged to have committed the crime.

Law enforcement did not have to ask for all 127 days of Mr. Carpenter's information. They ought to have asked for less data in case their suspicions of criminal activity proved unfounded. It is small comfort to the innocent citizen that police invaded his privacy on a good faith belief. It makes sense for legislation to impose a balancing test on the amount of electronic data authorities can access in a criminal investigation. The circumstances of each case will govern whether more information is needed, but authorities should not be engaged in a fishing expedition that needlessly embarrasses law-abiding citizens.

A good model for future privacy legislation is the Federal Wiretapping Statute, which generally prohibits anyone from intercepting phone communications.[354] The Federal Wiretapping Statute limits legal wiretapping to cases involving serious offenses, such as espionage or treason.[355] The Statute also requires wiretap applications to specify whether alternative investigative means are unavailable or too dangerous,[356] and the document must specify a duration.[357] A court issuing a wiretap order may only do so if probable cause of a crime exists,[358] there is probable cause that the investigated party will reveal evidence of

353. *Id.*; Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

354. 18 U.S.C. § 2511.

355. *See id.* § 2516(1)(a) (listing other offenses including nuclear facility sabotage, kidnapping, protecting trade secrets, piracy, sabotage, malicious mischief, and riots).

356. *Id.* § 2518(1)(c).

357. *Id.* § 2518(1)(d).

358. *Id.* § 2518(3)(a).

criminal activity,[359] and normal investigative measures are either unavailable or too dangerous.[360] Furthermore, a wiretap order has to terminate as soon as it is no longer needed.[361]

The Federal Wiretap Statute provides for criminal penalties for illegal wiretapping,[362] and the icing on the cake is that the individuals who wrongfully spy on others through illegal wiretapping can be sued individually for punitive damages and attorney fees.[363] This kind of statutory scheme would go a long way toward rectifying the public's privacy concerns in the area of stored electronic information. Such a statutory approach to CSLI would go a long way toward protecting privacy.

While statutory reform can impose important limits on technological intrusions not falling squarely into the Fourth Amendment's purview, constitutional change should also be enacted as a fail-safe. A constitutional amendment is a more permanent solution to privacy concerns because they are harder to repeal than statutory privacy protections. Constitutional amendments supersede any government attempts to abuse power as long as the judiciary counterbalances them. A privacy amendment should be broad enough that it need not anticipate all new technological innovations, and narrow enough that law enforcement is not crippled in its prosecution of crime. Perhaps a privacy amendment would be worded like this:

> Neither Congress nor the States shall establish a system of pervasive surveillance or monitoring of the general public, nor shall any individual be subjected to prolonged technology-assisted surveillance or monitoring except as strictly tailored to the interests of justice on the showing of probable cause.

Particularized suspicion must be required in a privacy amendment as a predicate for law enforcement to engage in prolonged technology-aided surveillance. It is fine for law enforcement to engage in stakeouts. The state does not have the resources to hire a person to watch every citizen at all times. It is a different matter if the state actor is a computer and the state is indiscriminately spying on everyone's online search history. Privacy is the "right to be left alone,"[364] and law enforcement should not be able to use

359. *Id.* § 2518(3)(b).
360. *Id.* § 2518(3)(c).
361. *Id.* § 2518(5).
362. *Id.* § 2511(4)(a).
363. *Id.* § 2520(b)(2)–(3).
364. *Privacy, Right of*, BARRON'S LAW DICTIONARY (6th ed. 2010).

advanced technologies to scan into homes or see into the bodies or chattels of law-abiding citizens. Law-abiding citizens should not be tracked at all hours by cameras or drones without a warrant. The government should be proscribed from imposing a system whereby all commercial transactions are tracked and society becomes effectively cashless. Furthermore, a constitutional amendment ought to balance the interests of law enforcement and the public with a standard that is not too strenuous on criminal investigations.

A constitutional amendment should resolve the problem that third parties' ownership of private information presents. The public rightly has a normative expectation of privacy concerning information shared with third parties in the course of daily life because there is a reasonable belief that the shared information will be used only in relation to the transaction. For example, a credit card user does not expect that the company will look through the purchases and publish a profile of that customer by name to the highest bidder. With that said, the customer understands that purchase information may be anonymized and sold, but this kind of limited privacy intrusion is a reasonable cost of doing business.

For law enforcement to obtain private customer information without probable cause through a subpoena to a third party, law enforcement should first craft a request that is narrowly tailored to the interests of justice. Law enforcement and government agencies should not be invited to a fishing expedition to trawl for information. The State should also be prohibited from creating databases on all its citizens by way of purchasing data on the market.

Statutes will fill in the gaps of an amendment. For example, one could create new tort causes of action for invasion of privacy by companies or private individuals, as demonstrated by the Federal Wiretap Statute. This would help in cases where a citizen does not endure prosecution, but still suffers an invasion of privacy.

The government can and always will abuse its power or make mistakes that infringe on the rights of others. However, an amendment to the Bill of Rights will provide an opportunity for the judiciary to step in and protect the people without acting as a quasi-legislative body. The Fourth Amendment protects the public from some intrusions, but not others.[365] The Constitution is sacred, and it is preferable to write a new chapter in this great work than to strain the words of the text; a new and

365. Katz v. United States, 389 U.S. 347, 350–51 (1967).

comprehensive privacy amendment to protect the human dignity of all citizens is long overdue.

V. CONCLUSION

Carpenter is a radical departure from established constitutional doctrine. It is a result-oriented opinion that confuses the law without settling it. Regardless of one's personal views on privacy, no accepted legal framework can support the Court's decision. The State may lawfully subpoena any information owned by third parties, provided the request is not unduly burdensome.

Mr. Carpenter was not searched under either of the Supreme Court's search tests. Because Mr. Carpenter did not own the CSLI, he cannot win under the trespass test. Alternatively, Mr. Carpenter did not have a reasonable expectation of privacy in CSLI voluntarily conveyed to the cell company by purchasing their services. The third-party doctrine imposes serious challenges to privacy in the modern day. It is unreasonable to insist that to have privacy, one must live a solitary life with the shades drawn.

In the end, privacy is such an important societal good that privacy rights should be memorialized by a combination of constitutional change and statutory reform. Alternatively, if the nation does not change the Constitution, some privacy protection by statute is better than nothing. However, with statutes or even the common law, what a legislature or judiciary can give, it can also take away. The variability in the Court's jurisprudence on privacy reveals this weakness.

It would be best to formally impose nationwide limitations on how much data can be obtained in criminal investigations without a search warrant. Natural law and universal values of rights do exist, but the judiciary cannot impose them.[366] The question is always whose version of natural law will apply, and for the purposes of a republic, the law "is not a brooding omnipresence . . . ."[367] The normative privacy values shared by the American people are fundamental to liberty, yet they must be implemented through the legislative process enshrined in the Constitution.

366. *See* Calder v. Bull, 3 U.S. 386, 399 (1798) (Iredell, J., concurring) (disputing the notion that the Supreme Court may strike down a law for violating natural law and noting even the wisest have disagreed on the matter of natural law).

367. S. Pac. Co. v. Jensen, 244 U.S. 205, 222 (1917) (Holmes, J., dissenting).