Fordham Urban Law Journal

Volume 47 | Number 5 Article 6

2020

Does Carpenter Put a Nail in Warrantless Police Searches of Smartphone Cell Site Location Information?

Christopher G. Trafford

DOES *CARPENTER* PUT A NAIL IN WARRANTLESS POLICE SEARCHES OF SMARTPHONE CELL SITE LOCATION INFORMATION?

Christopher G. Trafford[*]

[*] J.D. 2020, Fordham University School of Law; B.A. 2014, University at Albany, State University of New York. Thank you to Professors Eric Seidel and Andrew Kent for their invaluable insights during the writing of this Note, and to the editors and staff of the *Fordham Urban Law Journal* for their steadfast commitment to public policy and urban law issues. I am grateful to Fordham University for participating in the Yellow Ribbon Program, thereby providing a Veteran like myself the opportunity to continue serving our community, as well as all the friends and family who have supported me during my time as a law student.

INTRODUCTION

Certain modern law enforcement surveillance techniques lead to wrongful arrests and, arguably, infringe upon an individual's constitutional freedom from warrantless searches.[1] Indeed, such warrantless cell phone location searches on an individual's cell phone location are leading to wrongful incarceration.[2] For example, in December 2018, Avondale, Arizona, police arrested Jorge Molina after they ordered Google to turn over Molina's cell phone location records.[3] This information tied Molina's location to an earlier crime scene.[4] Molina was eventually cleared of his charges after police found the real culprit, but he will never be made whole from the reputational and emotional damage.[5] It is an open question today whether such warrantless location searches are constitutional. The Supreme Court and a number of states are currently weighing in on law enforcement's ability to warrantlessly track an individual's digital location records.

In the 2018 landmark case *Carpenter v. United States*, the Supreme Court decided that (1) an individual holds a legitimate expectation of privacy in that individual's cellular phone's "cell-site location information" (CSLI), and (2) warrantless law enforcement historical CSLI searches of one week or more violate the Fourth Amendment's protection against unreasonable searches and seizures.[6] CSLI is the information cell phones convey to nearby cell towers, which are then used to triangulate a person's position.[7] The *Carpenter* Court declined to rule whether real-time location surveillance or historical searches of less than one week require

---

1. *See generally* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/PJ3W-V8GK].

2. *See id.*

3. *See id.*

4. *See* Bree Burkitt, *Man Says Avondale Police Used Google Data to Wrongfully Arrest Him in 2018 Killing*, AZ CENTRAL (July 31, 2019), https://www.azcentral.com/story/news/local/southwest-valley/2019/07/31/jorge-luis-molina-says-avondale-police-used-google-data-wrongfully-arrest-him-murder-joe-knight/1873878001/ [https://perma.cc/G8EC-838N].

5. *See id.*

6. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

7. See *Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys*, ELEC. FRONTIER FOUND., https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf [https://perma.cc/YRH8-UU39] (last visited Sept. 10, 2020).

search warrants.[8] As a result, it is unknown whether current legislation that only requires "reasonable grounds"[9] to search CSLI sufficiently protects an individual's constitutional rights.

Legislators who enacted the outdated telecommunication laws could not have contemplated warrantless searches of an individual's location at virtually every moment.[10] Congress passed the Stored Communications Act in 1986, a whopping 14 years before the first cell phone would be equipped with GPS.[11] Ever-improving technological advances and societal reliance on cell phones made the *Carpenter* ruling inevitable. Justice Sotomayor remarked that, unlike previous decades, most people today consider their cell phone as more of an "appendage" than an electronic device.[12] Still, *Carpenter*'s narrow holding declined to rule on the constitutionality of *real-time* CLSI searches, as well as *historical* searches of less than one week.[13]

This Note seeks to examine *Carpenter* and, in doing so, best present possible solutions to protect an individual's real-time and historical CSLI. In Part I, this Note discusses the Supreme Court's recent opinion in *Carpenter v. United States*, with particular emphasis on the four dissents which imagine a different legal framework than the status quo. Part II traces the evolution of federal telecommunications legislation and common law doctrines regarding warrantless law enforcement searches, and the Fourth Amendment's protection against unreasonable searches and seizures.[14] Part III outlays the current judicial split amongst lower

---

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

9. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), https://cyber.harvard.edu/practicallawyering/Week9DOJECPAExcerpt.pdf [https://perma.cc/SM4L-KHPU] ("[T]he governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

10. *See generally* Mark Sullivan, *A Brief History of GPS*, PC WORLD (Aug. 9, 2012, 6:00 AM), https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html [https://perma.cc/74UP-CQQZ].

11. *See id.*

12. Alan Butler, *SCOTUS Justices Are Ready to Tackle Privacy Rights in the Digital Age*, HILL (Dec. 12, 2017, 7:00 AM), https://thehill.com/opinion/civil-rights/362901-scotus-justices-are-ready-to-tackle-privacy-rights-in-the-digital-age [https://perma.cc/G8M9-MFMK]; *see also* Amy Davidson Sorkin, *In* Carpenter *Case, Justice Sotomayor Tries to Picture the Smartphone Future*, NEW YORKER (Nov. 30, 2017), https://www.newyorker.com/news/our-columnists/carpenter-justice-sotomayor-tries-to-picture-smartphone-future [https://perma.cc/GRB4-SMEJ].

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

14. *See* U.S. CONST. amend. IV.

courts on how to treat real-time and historical CSLI searches post-*Carpenter*, as well as an initiative in some states to protect their citizens' location information from warrantless searches.

In conclusion, this Note advocates for states to individually adopt Justice Gorsuch's property classification of CSLI, thereby providing more protection against warrantless location searches than the federal government does, with the intent to influence the Supreme Court to adopt his approach eventually.

I. UNDERSTANDING *CARPENTER* AND EVOLVING POLICE SURVEILLANCE LAWS

Part I provides background information regarding *Carpenter* and the four dissents that accompanied Chief Justice Roberts's majority opinion. In particular, it reviews the applicable statutes and Supreme Court decisions that have brought us to today's Fourth Amendment crossroads. When law enforcement employs questionable modern surveillance methods, such as warrantless surveillance of an individual's cell phone location, governing law must be reviewed to determine its ongoing relevance and possible infringement upon the individual's constitutionally guaranteed freedom from "unreasonable searches and seizures."[15] Throughout this Note, it is important to keep in mind the Supreme Court's "sliding scale" approach to the Fourth Amendment, which provides a different, context-based threshold for what is considered "reasonable."[16]

A. Carpenter: Phone Thief Nabbed after His Own Cell Phone's Location Was Warrantlessly Searched

In 2018, the Supreme Court passed down its most impactful Fourth Amendment decision in years.[17] The Court granted certiorari in *Carpenter v. United States* to decide whether the Fourth Amendment protects against warrantless cell phone location record searches — which had never been classified as a person, paper, thing, or effect.[18] This holding calls into question whether current telecommunications legislation sufficiently protects an individual's CSLI from warrantless law

15. *See id.*

16. *See* Ronald J. Bacigal, *The Fourth Amendment in Flux: The Rise and Fall of Probable Cause*, 1979 U. ILL. L.F. 763, 765 (1979).

17. *See generally* Carpenter v. United States*: Whether the Fourth Amendment Permits the Government to Obtain Six Months of Cell Phone Location Records Without a Warrant*, ELEC. PRIV. INFO. CTR., https://epic.org/amicus/location/carpenter/ [https://perma.cc/JH9L-HZ84] (last visited Sept. 10, 2020).

18. *See generally Carpenter*, 138 S. Ct. at 2206.

enforcement searches. Law enforcement may currently search this data if they have reasonable suspicion, which is a lower standard than probable cause that the Fourth Amendment demands.[19] But in exchange, searching CSLI allows law enforcement to identify suspects more efficiently and take them into custody. Fourth Amendment enthusiasts closely followed *Carpenter v. United States*, keenly aware that *Carpenter*'s holding and extrapolated rationale could result in dramatic consequences affecting an individual's right to be free from warrantless location searches.[20]

i. RadioShack Robbery: An Unlikely Digital Privacy Battleground

Timothy Carpenter is now the face of digital privacy. He arrived at this position when he received a 116-year sentence after police searched his CSLI without a warrant.[21] Many, including nationally recognized law professor Orin Kerr, have scrutinized the circumstances leading to Carpenter's arrest and conviction.[22] His story began in April 2011, when law enforcement investigated a string of robberies from nine different RadioShack and T-Mobile stores across Ohio and Michigan.[23] They quickly arrested four suspects, one who confessed to the robberies and implicated 15 accomplices.[24] This informant voluntarily provided the Federal Bureau of Investigation with a list of his co-conspirators' cell

19. *See* Sean Fernandes, *Supreme Court Addresses Stored Communications Act Cases*, AM. BAR ASS'N (Feb. 15, 2019), https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2018/supreme-court-addresses-stored-communications-act-cases/ [https://perma.cc/YE6J-PTDX].

20. *See, e.g.*, Rebecca Kielty, Carpenter v. United States*: Impacts on Privacy Legislation*, NAT'L CONSUMERS LEAGUE (June 2018), https://www.nclnet.org/carpenter_decision [https://perma.cc/LEC5-KYFR] ("You're thinking, 'And? I'm not accused of armed robbery,' but it's bigger than Timothy Carpenter. The *Carpenter* decision affects all of us, and in essence redefines government searches in a digital age.").

21. *See* Brandi Buchman, *High Court Bends for Digital Privacy in Cell-Search Case*, COURTHOUSE NEWS SERV. (Nov. 29, 2017), https://www.courthousenews.com/high-court-bends-for-digital-privacy-in-cell-search-case/ [https://perma.cc/SGD3-8WJE].

22. *See, e.g.*, Orin Kerr, *Does* Carpenter *Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/3YXN-58UZ].

23. *See* Rebecca Heilweil, *A Guy Who Stole Phones from Radioshack Could Be the Next Face of Digital Privacy*, FORBES (June 20, 2018, 1:10 PM), https://www.forbes.com/sites/rebeccaheilweil1/2018/06/20/a-guy-who-stole-phones-from-radioshack-could-be-the-next-face-of-digital-privacy/#4d54bed42e5f [https://perma.cc/A6H3-799E].

24. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

phone numbers.[25] Law enforcement also uncovered a number of additional cell phone numbers that the informant called around the time of the robberies, but which the informant did not volunteer.[26] Timothy Carpenter's number was among those.[27]

With this new information, the Government obtained court orders pursuant to the Stored Communications Act (SCA), compelling the suspects' cellular providers to turn over their location records.[28] The SCA permits law enforcement to obtain reports from cellular providers by court order where there are "reasonable grounds" for suspicion.[29] MetroPCS and Sprint (Carpenter's wireless carriers at the time) dutifully turned over 127 days of Carpenter's CSLI to investigators.[30] Currently, triangulating this CSLI can pinpoint a person's location to within five to ten feet, and this technology is ever-improving.[31] Carpenter's CSLI allowed the prosecution to catalog and map out exactly 12,988 of his location points and times, which averages to about 101 data points per day.[32] This compilation placed Carpenter at the scene and time of each robbery.[33] Thereafter, Timothy Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence.[34] Carpenter moved to suppress the CSLI evidence against him on Fourth Amendment grounds.[35] The United States District Court for the Eastern District of Michigan denied Carpenter's motion to suppress the evidence, and the United States Court of Appeals for the Sixth Circuit upheld the district court's ruling.[36] The Supreme Court granted certiorari.[37]

---

25. *See id.*

26. *See id.*

27. *See id.*

28. *See* 18 U.S.C. § 2703(d) (2019).

29. *See* Fernandes, *supra* note 19.

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

31. *See Cell Phone Location Tracking: A National Association of Criminal Defense Lawyers (NACDL) Primer*, NAT'L ASS'N CRIM. DEF. LAWS. & SAMUELSON L., TECH., & PUB. POL'Y CLINIC (June 7, 2016), https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/UV8J-HL4B].

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

33. *See id.*

34. *See id.*

35. *See id.* The Fourth Amendment protects individuals from "unreasonable" searches and seizures. *See* U.S. CONST. amend. IV.

36. *See Carpenter*, 138 S. Ct. at 2206.

37. *See id.* at 2213.

ii. Modern Technology "[I]s an Open Box. We Know Not Where We Go"[38]

In another 5–4 ruling during this politically-charged era,[39] the Supreme Court held that law enforcement's CSLI collection constituted a Fourth Amendment "search," thus requiring a warrant secured by probable cause. [40] The *Carpenter* Court held that the Government's reasonable grounds of suspicion court order was insufficient to conduct a CSLI search.[41] The Court purposely ruled narrowly, however, careful not to disturb prior Supreme Court decisions regarding law enforcement surveillance and the Fourth Amendment.[42] The Court also declined to address modern surveillance tactics, such as security cameras.[43] As a result, lower courts remain split on whether particular warrantless police searches are "reasonable," especially now that individuals can be tracked with almost pinpoint precision at all times.[44] And this technology is only improving and getting more accurate.

Chief Justice Roberts wrote *Carpenter*'s majority opinion,[45] which was followed by four separate dissents from the other conservative Justices. The Chief Justice held that law enforcement's access to Carpenter's CSLI indeed constituted a Fourth Amendment search because it violated Carpenter's "legitimate expectation of privacy in the record of his physical movements."[46] In other words, law enforcement's warrantless search of Carpenter's CSLI for seven days violated his "reasonable expectation of privacy" that the Fourth Amendment guarantees.[47] The Court equated a CSLI search to attaching an ankle monitor to the phone's

---

38. Transcript of Oral Argument at 34, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf [https://perma.cc/96FC-JEU3].

39. Chief Justice Roberts sided with the four liberal-leaning Justices to form a majority. *See* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/KQ4L-AXKC].

40. *See* Kate Fazzini, *Supreme Court Ruling Requiring Warrant for Cellphone Searches Could Lead to a Flood of Lawsuits*, CNBC (June 25, 2020, 7:18 PM), https://www.cnbc.com/2018/06/25/privacy-scotus-cell-data-carpenter-v-usa.html [https://perma.cc/L863-NFCL].

41. *See id.*

42. *See Carpenter*, 138 S. Ct. at 2220–21.

43. *See id.*

44. See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012).

45. *See Carpenter*, 138 S. Ct at 2211.

46. *Id.* at 2217.

47. *See* Kerr, *supra* note 22.

user.[48] The analogy here is that since both a cell phone and ankle monitor are on the person at all times, a search is inherently intrusive and requires a warrant. However, the Court was careful to not "embarrass the future" by creating a rule that would quickly become obsolete as technology advanced.[49] It declined to provide "judicial answers [regarding CSLI] which at best can deal only in a truncated way with problems sufficiently difficult even for legislative statesmanship."[50] For this reason, the Court held that a CSLI search of seven days or more constitutes a Fourth Amendment search.[51]

iii. This CSLI Investigation Constituted a Search, but What about Others?

Due to *Carpenter*'s narrow holding, it is only a matter of time before law enforcement surveillance technology reaches the Supreme Court again.[52] Therefore, an analysis of *Carpenter*'s separate dissents is necessary to consider a more permanent solution. Dissents and concurrences sometimes serve as persuasive authority in Fourth Amendment jurisprudence and may guide future majority opinions.[53] Resolving future issues with a reasoned and well-informed holding will require much reconciliation of competing interests, like out-of-date telecommunications statutes and different Supreme Court Justices' approaches. Otherwise, the next Supreme Court case on law enforcement surveillance risks becoming obsolete over time, over-inclusive, under-inclusive, or even an infringement upon an individual's freedom from "unreasonable" searches and seizures. Indeed, the Court and legislature's inertia to act definitively results in law enforcement, with little checks on its discretion, to warrantlessly track individuals. Although *Carpenter* recognizes these risks and therefore limits its applicability, previously unforeseeable instances are now foreseeable. Yet issues surrounding real-time and historical CSLI searches of less than seven days are currently left unresolved because it remains unclear the extent to which law enforcement can constitutionally surveil an

48. *See Carpenter*, 138 S. Ct. at 2218.

49. *See id.* at 2220.

50. Nw. Airlines v. Minnesota, 322 U.S. 292, 300 (1944).

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

52. *See* Vanessa Blum, *What's Next for Digital Privacy? New Clashes over the Fourth Amendment*, LAW.COM (Mar. 7, 2019, 4:36 PM), https://www.law.com/therecorder/2019/03/07/whats-next-for-digital-privacy-new-clashes-over-the-fourth-amendment/?slreturn=20200505113737 [https://perma.cc/3EZM-F6XE].

53. *See* Vanessa Baird & Tonja Jacobi, *How the Dissent Becomes the Majority: Using Federalism to Transform Coalitions in the U.S. Supreme Court*, 59 DUKE L.J. 183, 183 (2009).

individual's CSLI. For this reason, a definitive answer to the constitutionality of warrantless CSLI searches with clear demarcations of law enforcement's warrantless search capabilities, along with the individual's Fourth Amendment right to be free from warrantless, intrusive surveillance, must be provided.

1. Justice Kennedy (Joined by Justices Thomas and Alito): Treat CSLI as a Business Record

Justice Kennedy advocated for treating warrantlessly obtained CSLI like other types of business records, such as bank or accounting records.[54] This approach defers to the "Third Party Doctrine," which states that searching location records that are "possessed, owned, and controlled" by service providers does not infringe upon an individual's right from unreasonable searches under the Fourth Amendment.[55] Two cases before the Supreme Court, *United States v. Miller*[56] and *Smith v. Maryland*,[57] set forth this doctrine, which states that voluntarily sharing information with third parties negates any reasonable expectation of privacy in that information.[58] Specifically, *Miller* held that people have no Fourth Amendment privacy rights in financial records that their bank stores, whereas *Smith* permitted a warrantless search where police utilized a pen register to monitor a suspect's outgoing call data.[59]

Still, Justice Kennedy appreciated the possibility that advanced surveillance capabilities may infringe on an individual's Fourth Amendment guarantee against unreasonable searches and seizures.[60] Regarding this, he remarked that "property norms and expectations of privacy . . . [are] difficult to determine during periods of rapid technological change. In those instances, and where the governing legal standard is one of reasonableness, it is wise to defer to legislative

---

54. *See Carpenter*, 138 S. Ct. at 2223 (Kennedy, J., dissenting).

55. *See id.*; *infra* Section I.B.ii. The Third Party Doctrine holds that voluntarily sharing information with third parties negates any reasonable expectation of privacy in that information. This effectively negates any right in the individual's own CSLI once the wireless carrier receives it. *See infra* Section I.B.ii.

56. 425 U.S. 435 (1976).

57. 442 U.S. 735 (1979).

58. *See* Heilweil, *supra* note 23.

59. *See* John Villasenor, *What You Need to Know About the Third Party Doctrine*, ATLANTIC (Dec. 10, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ [https://perma.cc/3DCK-GFHX]. A pen register is a device a telephone company installs to record the phone numbers an individual dials. *See Pen Register*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/NDQ4-RKSP] (last visited Sept. 10, 2020).

60. *See Carpenter*, 138 S. Ct. at 2233 (Kennedy, J., dissenting).

judgments like . . . the Stored Communications Act."[61] This approach gives deference to the legislature, which is democratically accountable and therefore better situated to gauge what society would deem as a "reasonable" warrantless search than a majority of unelected Supreme Court Justices.

2. Justice Thomas: The Fourth Amendment's Text Does Not Protect CSLI

Justice Thomas's main point of objection with the *Carpenter* majority opinion was that the Supreme Court implemented the "reasonable expectation of privacy test" developed in the 1967 opinion *Katz v. United States*.[62] Justice Thomas believed that the *Katz* test from Justice John Marshall Harlan's concurrence lacked grounding in the Fourth Amendment's text and original meaning.[63] To illustrate this point, Justice Thomas noted how the word "privacy" is absent from the Fourth Amendment, as well as the Framers' original intent after a historical review. [64] Justice Thomas argued that these two points show that the Fourth Amendment does *not* protect privacy.[65] He stated that "[b]y defining 'search' to mean 'any violation of a reasonable expectation of *privacy*,' the *Katz* test misconstrues virtually every one of [the Fourth Amendment's] words."[66] Justice Thomas then reviewed the dictionary meaning of "search" from an edition dating back to 1828 to understand the Framers' actual intent when drafting the Fourth Amendment.[67] He urged the Court to dismiss the *Katz* privacy test altogether.[68]

Justice Thomas also disagreed with Carpenter's attempt to categorize his CSLI as a Fourth Amendment "paper" to invoke a property right in his location.[69] Justice Thomas explained that an individual has never held a property right in cell-site records "under the law of any jurisdiction at any point in American history."[70]

---

61. *Id.*

62. 389 U.S. 347 (1967).

63. *See Carpenter*, 138 S. Ct. at 2236 (Thomas, J., dissenting).

64. *See id.* at 2238.

65. *See id.*

66. *Id.* (emphasis added).

67. *See id.* At the time, the ordinary meaning of "search" was "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief." *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001)).

68. *See id.* at 2244.

69. *See id.* at 2242.

70. *Id.*

3. Justice Alito (Joined by Justice Thomas): The Fourth Amendment's Intent Does Not Protect CSLI

Justice Alito similarly criticized the inconsistency between "property" that the Fourth Amendment should protect — as determined by analyzing the ordinary meaning of the Amendment's text — and Justice Roberts's majority opinion.[71] Justice Alito emphasized the Amendment's plain meaning and the Framers' intent should be dispositive in concluding the Constitution does not protect against warrantless CSLI searches.[72] He then quoted Justice Hugo Black's dissent in *Katz*: "The Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates."[73] In other words, as originally understood by the Framers, "the Fourth Amendment would not have applied at all to the methods that law-enforcement officials use to obtain documents" to include warrantless CSLI searches.[74]

Justice Alito also emphasized that the Government followed the well-established Third Party Doctrine to receive Carpenter's CSLI.[75] However, now that the Supreme Court declared unconstitutional this law enforcement search, all searches longer than one week are similarly rendered unconstitutional.[76] It remains to be seen whether searches of lesser duration are unconstitutional, as the Supreme Court "has offered no meaningful limiting principle, and none is apparent"[77] — suggesting that Justice Alito is apprehensive *Carpenter* will impede on current law enforcement policies, which allow searches under reasonable grounds instead of probable cause.[78]

4. Justice Gorsuch: Instill an Individual Property Right in CSLI

Justice Gorsuch's dissent urges future defendants to make a property-based argument to protect their CSLI, which the Supreme Court

---

71. *See id.* at 2247 (Alito, J., dissenting).

72. *See id.* at 2250.

73. *See id.* at 2251 (quoting Katz v. United States, 389 U.S. 347, 367 (1967) (Black, J., dissenting)).

74. Amy Howe, *Opinion Analysis: Court Holds That Police Will Generally Need a Warrant for Sustained Cellphone Location Information (Updated)*, SCOTUSBLOG (June 22, 2018, 6:01 PM), https://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/ [https://perma.cc/95QL-6HDN].

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

76. *See id.* at 2266–67 (Gorsuch, J., dissenting).

77. *Id.* at 2256 (Alito, J., dissenting).

78. *See id.*

may later classify as "person, house, paper, and effect" under the Fourth Amendment.[79] Of course, this is a novel idea shown by Justice Thomas's and Justice Alito's respective dissents, which each argue that the Fourth Amendment explicitly does not protect CSLI from warrantless searches.[80] Nonetheless, the idea of endowing Fourth Amendment protection in new technology is consistent with Justice Gorsuch's previous Tenth Circuit opinions.[81]

Justice Gorsuch argued that an individual's CSLI might "qualify as *his* papers or effects under existing law"[82] under the Fourth Amendment for two reasons: (1) the statutory Privacy of Customer Information Act provides an individual CSLI property right, and (2) technology is increasingly used for storing information in the modern era, much like a "paper" was during the eighteenth century, when the Fourth Amendment was written.[83]

iv. Justice Gorsuch's Originalist Argument Regarding Property Rights in CSLI

Justice Gorsuch argued that the Fourth Amendment protects against warrantless law enforcement searches of an individual's CSLI. Although previous Supreme Court terms and some sitting Justices today hesitate to adapt the Fourth Amendment to modern surveillance technology, Justice Gorsuch shows no such hesitation.[84] Justice Gorsuch uses the following statutory and contextual arguments to bolster his claim.

---

79. *See id.* at 2272 (Gorsuch, J., dissenting).

80. *See id.* at 2237–44, 2264; *supra* Sections I.A.iii.b–c.

81. *See* United States v. Ackerman, 831 F.3d 1292, 1295 (10th Cir. 2016) (holding that opening an email file constituted a Fourth Amendment "search").

82. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

83. *See id.* at 2267–68, 2272 ("The Fourth Amendment protects 'the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures.' True to those words and their original understanding, the traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment. Though now often lost in *Katz*'s shadow, this traditional understanding persists. . . . Yes, the telephone carrier holds the information. But 47 U.S.C. § 222 designates a customer's cell-site location information as 'customer proprietary network information' (CPNI), § 222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves.'").

84. *See* Jim Harper, *Common-Law Originalism in Tech Policy, Too*, AM. ENTER. INST. (Jan. 28, 2020), https://www.aei.org/technology-and-innovation/common-law-originalism-in-tech-policy-too/ [https://perma.cc/8FKL-DAHK].

1. Privacy of Customer Information Act

Justice Gorsuch's statutory argument to vest a property right in CSLI comes from Congress. The Privacy of Customer Information Act requires that (1) federal statutes regard CSLI as "*customer proprietary* network information,"[85] (2) carriers are generally forbidden from using CSLI without the customer's consent, (3) carriers must disclose CSLI upon the customer's consent, and (4) Congress provide individuals with a cause of action for claims brought against non-compliant carriers.[86] These interests signal a personal interest in the individual's own CSLI, culminating in a Fourth Amendment property right.[87] Therefore, Justice Gorsuch posited, "[p]lainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right."[88] Unfortunately, Timothy Carpenter made a fatal error in not raising or preserving this statutory defense in *Carpenter*.[89] Lower courts and law enforcement must now wait for Supreme Court guidance about the constitutionality of other warrantless CSLI searches because "[Carpenter] forfeited Fourth Amendment arguments based on positive law by failing to preserve them."[90]

2. Modern Technology Has Fundamentally Changed How America Stores Information

Today, as opposed to 1791 or even 20 years ago, we rely upon technology to conduct almost everything in our lives, from important business to mundane tasks. The overwhelming majority of people in the United States rely on their cell phones to navigate, store confidential medical and financial information, and even conceal their most personal and intimate photos and communications.[91] Due to this foundational

85. 47 U.S.C. § 222 (2012) (emphasis added).

86. *See id.*

87. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

88. *See id.*

89. *See id.*

90. *Id.*

91. *See* Kielty, *supra* note 20 ("Think of your relationship with your cell phone. According to Pew, 95 percent of Americans now own one. The same study found that for one in five of us, our smartphone is our sole source of Internet service. We carry them to work, to school, to our homes, and to meet up with friends. They go with us to our meetings, appointments, and vacations. They are a key vector through which we're understood. Part of that is an unprecedented ability to locate us. When 95 percent of us are moving and communicating with our phones, and when 20 percent of us are using them as our only personal Internet connection, government access to when and where we use cell phones becomes an inroad to very intimate surveillance.").

societal change, Justice Gorsuch argued that the Fourth Amendment should protect personal information residing in cellular devices like it does for constitutionally-protected information in one's nightstand. [92] He noted how documents which, "in other eras, we would have locked safely in a desk drawer or destroyed — now reside on third party servers."[93] According to Justice Gorsuch, because they contain the same information, "virtual" documents that constitute "papers" deserve Fourth Amendment protection.

v. Justice Gorsuch's Case against the Third Party Doctrine

Under the Third Party Doctrine, individuals lose any property interest in cellular information — if they ever had one — once the signal reaches their wireless carrier.[94] The Supreme Court held that individuals do not have a legitimate "expectation of privacy" in such information because they volunteered the information to their service provider.[95] As a result, the Fourth Amendment does not protect against warrantless searches of CSLI, banking records, and other business records that a third party holds.[96] However, Carpenter failed to preserve the argument that CSLI may be categorized as "property" under the Fourth Amendment.[97] If he had employed that defense, the Supreme Court could very well find that CSLI deserves Fourth Amendment protection, rendering all warrantless CSLI searches unconstitutional. This is because applying the Third Party Doctrine's lower standard to searches that demand probable cause warrants would insufficiently protect the individual from unreasonable warrantless searches.

Justice Gorsuch made the property argument that "[e]ntrusting your [property] to others is a *bailment*,"[98] defined as the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose."[99] Under a property law lens, an

---

92. *See id.* at 2271. "[T]his Court has recognized that using that technology to look inside a home constitutes a Fourth Amendment 'search' of that 'home' no less than a physical inspection might." *Id.*

93. *Id.* at 2262.

94. *See infra* Section I.B.

95. *See infra* Section I.B.ii.

96. *See generally* United States v. Miller, 425 U.S. 435 (1976) (holding that bank records are not protected by the Fourth Amendment); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (holding that law enforcements' use of a pen register is not a "search" within the meaning of the Fourth Amendment).

97. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

98. *Id.* at 2268.

99. *Id.* (internal quotations omitted) (citing BLACK'S LAW DICTIONARY (10th ed. 2014)).

individual would not lose interest in their CSLI after it is transmitted to their cellular provider. "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, *wherever they may be*."[100] Therefore, any CSLI inspection would possibly require a probable cause warrant to comport with the Fourth Amendment.

B. Applicable Statutes and Common Law Concerning Warrantless Police Surveillance

Federal statutes and Supreme Court decisions primarily govern the intersection of modern law enforcement surveillance techniques and the Fourth Amendment's protection from unreasonable searches and seizures. Undoubtedly, some of our telecommunication laws were drafted without CSLI in mind. Yet the Supreme Court must apply these laws to modern surveillance situations where technology has evolved so drastically that searches of invasive location searches, including inside of "purses, pockets, briefcases, and backpacks," are possible without contact.[101] The following cases and statutes help explain the Supreme Court's and Congress' understanding of societal expectations regarding when warrantless searches are reasonable.

i. Katz v. United States

Katz v. United States established a "balancing test" to decide whether an individual's right to privacy is protected in particular situations.[102] The Supreme Court granted certiorari to determine whether a "bugged" phone booth infringed upon an individual's Fourth Amendment right to be free from unreasonable searches and seizures.[103] This case is salient today because "[t]he long arm of *Katz* reaches into recent debates over mass data collection and GPS tracking. Indeed, in an age of increasing digital technology, the principle that the Fourth Amendment 'protects people, not places' is more consequential than ever."[104]

---

100. *Ex parte* Jackson, 96 U.S. 727, 733 (1878) (emphasis added).

101. Brief for the Electronic Frontier Foundation et al. as Amici Curiae in Opposition of the Government's Request for Review at 18, *in re* United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585 (2007) (No. 2:07-MJ-00524).

102. 389 U.S. 347 (1967).

103. *See id.*

104. Nicandro Iannacci, Katz v. United States*: The Fourth Amendment Adapts to New Technology*, NAT'L CONST. CTR. (Dec. 18, 2018), https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology [https://perma.cc/68NY-BUTZ].

In *Katz*, the Supreme Court held that the Fourth Amendment applies to oral statements in the same way that it applies to tangible objects.[105] Regarding privacy, the Court stated: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[106]

Justice Harlan's *Katz* concurrence set forth the "reasonable expectation of privacy" test now used to determine whether warrantless law enforcement surveillance constitutes a "search" and thus requires a probable cause warrant.[107] One possible drawback of this test is that it lacks bright-line rules for the judiciary to apply.[108] Because of this discretion, the reasonable expectation of privacy test "has haunted Fourth Amendment jurisprudence all these decades, partly because no one is entirely sure what it means in different fact situations raised by different cases."[109] This test does, however, respond to "[l]egitimation of expectations of privacy [that] by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[110] For example, when the sliding scale approach is applied to the home,[111] owners and tenants "almost always" have a reasonable expectation of privacy.[112] On the other hand, visitor rights are more uncertain because "it's not enough to simply happen to be somewhere in order to contest a search, but [one does not] have to have a strict property interest in the place either."[113] The fact that different individuals can have different expectations of privacy in the same area results in much judicial discretion when it comes to reasonable expectations of privacy.

---

105. *See id.*

106. *Katz*, 389 U.S. at 351 (internal citations omitted).

107. *See id.* at 361.

108. *See* Andrew Crocker, *The Supreme Court Says Your Expectation of Privacy Probably Shouldn't Depend on Fine Print*, ELEC. FRONTIER FOUND. (May 15, 2018), https://www.eff.org/deeplinks/2018/05/supreme-court-says-your-expectation-privacy-probably-shouldnt-depend-fine-print [https://perma.cc/Q6KV-4EES].

109. Mike Godwin, *What's Next for the Reasonable Expectation of Privacy?*, SLATE (June 27, 2018, 3:28 PM), https://slate.com/technology/2018/06/after-the-supreme-courts-carpenter-ruling-where-is-the-reasonable-expectation-of-privacy-heading.html [https://perma.cc/Q825-C5E5].

110. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

111. *See* Crocker, *supra* note 108. *See generally, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003) (invalidating a Texas statute that made it a crime for same-sex persons to engage in sexual conduct. Such laws were unconstitutional as applied to adults in the privacy of their homes).

112. *See* Crocker, *supra* note 108 (quoting Minnesota v. Carter, 525 U.S. 83 (1998)).

113. *Id.*; *see also* Minnesota v. Olsen, 495 U.S. 91, 93 (1990) (holding that overnight guests can contest a police search).

This discretion can lead to good-faith differences in what modern warrantless surveillance searches are reasonable.

ii. Third Party Doctrine

The Third Party Doctrine permits law enforcement to warrantlessly collect an individual's information from third party businesses, like cellular providers and banks.[114] The Supreme Court established the doctrine through a duo of 1970s cases,[115] and the Government in *Carpenter* relied on this doctrine to justify Carpenter's warrantless CSLI search.[116]

This doctrine is now applied to modern forms of information to surveil other third party records.[117] This is true notwithstanding our current technological revolution, the likes of which have not been seen since perhaps when Gutenberg invented the printing press.[118] As a result, a number of modern law enforcement surveillance tactics have come under scrutiny as law enforcement are now able to access vast quantities of data, which the legislature simply could not foresee when adopting the Stored Communications Act.[119] "[D]igitization and technological advances [have] increasingly placed the [Third Party] doctrine under pressure, as an increasing amount of potentially revealing information is now in the hands of third parties."[120] This suggests that reasonable societal expectations of privacy are changing, which is why some have called the

---

114. *See* Matthew Feeney, *Surveillance Tech Still a Concern After* Carpenter, CATO INST. (June 25, 2018, 12:44 PM), https://www.cato.org/blog/surveillance-tech-still-concern-despite-carpenter [https://perma.cc/68HP-VTUM].

115. The two cases establishing the Third Part Doctrine, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), hold that voluntarily sharing information with third parties negates any reasonable expectation of privacy in such information. *See* Heilweil, *supra* note 23.

116. *See* Jim Garland & Alexander Berengaut, *Supreme Court's* Carpenter *Decision Requires Warrant for Cell Phone Location Data*, COVINGTON: INSIDE PRIVACY (June 22, 2018), https://www.insideprivacy.com/data-privacy/supreme-courts-carpenter-decision-requires-warrant-for-cell-phone-location-data/ [https://perma.cc/7T2M-QHX8].

117. *See* Christopher C. Fonzone et al., Carpenter *and Everything After: The Supreme Court Nudges the Fourth Amendment into the Information Age*, 58 INFRASTRUCTURE 3, 3 (2019).

118. *See* Jeremiah Dittmar, *Information Technology and Economic Change: The Impact of the Printing Press*, VOXEU (Feb. 11, 2011), https://voxeu.org/article/information-technology-and-economic-change-impact-printing-press [https://perma.cc/DQW5-7TCL] ("The movable type printing press was the great revolution in Renaissance information technology and arguably provides the closest historical parallel to the emergence of the internet . . . .").

119. *See* Fonzone et al., *supra* note 117, at 4–5.

120. *Id.* at 3.

Third Party Doctrine, in the context of law enforcement's vastly improved surveillance capabilities, into question.[121]

In *Carpenter*, the Sixth Circuit held on appeal that Timothy Carpenter did not have a "reasonable expectation of privacy" in his physical location as determined by CSLI.[122] The Supreme Court, however, overturned the circuit court.[123] The Supreme Court explicitly ruled narrowly, and the only bright-line rule established was that collecting seven days or more of historical CSLI requires a warrant.[124] This holding creates a compliance issue because lower courts must decide whether the Third Party Doctrine applies to real-time CSLI searches and CSLI searches of less than seven days.

iii. Stored Communications Act of 1986

Congress passed the Stored Communications Act of 1986 (SCA) to regulate the exponential growth of modern technology (at this time, e-mail was becoming prominent).[125] The SCA provides procedural steps the government must take to obtain, inter alia, CSLI from third-party service providers like Verizon or T-Mobile.[126] The SCA permits the government to compel disclosure of an individual's telecommunication records when two conditions are satisfied: (1) the prosecution presents to the court "specific and articulable facts showing that there are reasonable grounds to believe that the records sought are (2) relevant and material to an ongoing criminal investigation."[127] When both prongs are met, a judge may issue a "Section 2703(d) Order"[128] that law enforcement uses to compel service providers to turn over stored communications relating to a suspect.[129]

---

121. *See* Kerr, *supra* note 22.

122. *See* Feeney, *supra* note 114.

123. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

124. *See id.* at 2217 n.3.

125. *See* 18 U.S.C. § 2703(d).

126. *See* Mariam Morshedi, *The Stored Communications Act of 1986*, SUBSCRIPT L. (Jan. 29, 2018), https://www.subscriptlaw.com/blog/stored-communications-act-origins [https://perma.cc/V3FS-5G4S].

127. *Carpenter*, 138 S. Ct. at 2212 (internal quotations omitted) (quoting § 2703(d)).

128. *See* Brief of Amici Curiae, *supra* note 101, at 14.

129. *See* Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, LAWFARE (June 22, 2018, 2:05 PM), https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states [https://perma.cc/93FV-AMD4].

iv. The SCA's "Reasonable Grounds" of Suspicion Standard

Under the SCA, the standard the judiciary applies is "considerably lower than the probable cause required for a typical warrant."[130] In *Carpenter*, the Government met the reasonable grounds standard by presenting testimony from an informant that identified several accomplices' cell phone numbers.[131] With that, law enforcement received judicial authorization to compel Carpenter's cell service providers to turn over his location information.[132] The prosecution received 12,898 of Carpenter's location points over 127 days, which averages to around 101 data points per day.[133]

In *Carpenter*, Chief Justice Roberts declared that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," regardless of whether government surveillance or provider data collection created those records.[134] Therefore the above CSLI search required a probable cause warrant, which the police did not obtain. As a result, the Court unequivocally held that the warrantless law enforcement search infringed upon Carpenter's Fourth Amendment rights, even though law enforcement satisfied the SCA's two-part test and received judicial authorization.[135] Law enforcement simply failed to meet the more protective "probable cause" standard the Fourth Amendment requires.[136]

The *Carpenter* Court held the Government needs a probable cause warrant for historical CSLI searches of one week or more.[137] This negates the SCA's two-part test, at least as it pertains to longer historical CSLI searches.[138] "Reasonable" societal expectations about warrantless searches superseded the SCA for this type of search once the Fourth Amendment was implicated.[139]

v. United States v. Jones

In *Carpenter*, the Supreme Court reaffirmed precedent from the 2012 police surveillance case *United States v. Jones* — at issue was whether

130. *Id.*
131. *See Carpenter*, 138 S. Ct. at 2212.
132. *See id.*
133. *See id.*
134. *Id. at* 2217.
135. *See id. at* 2221.
136. *See id.* ("[T]he Government's obligation is a familiar one — get a warrant.").
137. *See id.*
138. *See supra* Section I.B.iii.
139. *See* Fernandes, *supra* note 19.

warrantless law enforcement surveillance infringed upon an individual's Fourth Amendment protections.[140] The Court ultimately held that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[141]

In *Jones*, law enforcement attached a GPS tracker to a suspect's vehicle for one month without following the precise instructions set forth in the warrant.[142] In 28 days, they collected over 2,000 pages of Jones's location data.[143] With such vast access to Jones's location, investigators learned all of his movements and intimate aspects of his life.[144] Not unlike finance's "mosaic theory," law enforcement was able to construct a comprehensive illustration of Jones's habits by analyzing the aggregated data from the locations he visited.[145] The Government contended this action was permissible for two reasons: (1) there is no reasonable expectation of privacy on public roads; and (2) the Fourth Amendment only protects against trespass upon personal property.[146]

The Justices met the Government's argument against requiring a warrant for GPS — stating law enforcement could have followed Jones around on the public thoroughfares without a warrant — with criticism.[147] During oral arguments, Chief Justice Roberts asked the Government whether it believed that "there would also not be a search if [it] put a GPS device on all of [the Justices'] cars [and] monitored [their] movements for a month?"[148] Similarly, Justice Breyer quipped that if the Government won, "there is nothing to prevent the police or the government from monitoring 24 hours a day the public movement of every citizen of the United States."[149] The search in *Jones* failed to comport with societal notions regarding reasonableness and the Fourth Amendment.

---

140. *See* United States v. Jones, 565 U.S. 400, 402 (2012).

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

142. *See id.* at 2215.

143. *See Jones*, 565 U.S. at 403.

144. *See id.* at 416.

145. *See* Ashley Jacques, *The Mosaic Theory,* Riley, *and the Legacy of* Jones, INFO. L. INST.: BLOG (Mar. 12, 2015, 4:38 PM), https://blogs.law.nyu.edu/privacyresearchgroup/2015/03/the-mosaic-theory-riley-and-the-legacy-of-jones/ [https://perma.cc/5H58-3YGC]; *see also* Christian Bennardo, Note, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 Fordham L. Rev. 2385 (2017).

146. *See Jones*, 565 U.S. at 406.

147. *See* Transcript of Oral Argument at 9–10, United States v. Jones, 565 U.S. 400 (No. 10-1259).

148. *Id.* at 9.

149. *Id.* at 13.

The *Jones* Court unanimously held that law enforcement conducted a Fourth Amendment search by applying a GPS tracker onto a suspect's car without following the exact procedures set forth in the probable cause warrant.[150] However, the Justices disagreed on why this particular law surveillance is a "search," an issue also in *Carpenter*.[151] Did surveillance become a search because of the physical invasion of the vehicle, as Chief Justice Roberts and Justices Scalia, Kennedy, Sotomayor, and Thomas believed?[152] Or perhaps the search occurred because Jones's "reasonable expectation of privacy" was violated under *Katz*, as Justices Alito, Breyer, Ginsburg, and Kagan found.[153]

Jones is known partly for Justice Sotomayor's concurrence, which proposed that a Fourth Amendment "search" occurs anywhere the government encroaches upon reasonable societal expectations of "privacy," not only during trespass onto property.[154] In response to Justice Alito's concurrence about physical property intrusion, she stated that "society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalog every single movement of an individual's car for a very long period."[155] The *Carpenter* majority later emphasized this purview.[156] The struggle to delineate between reasonable warrantless searches and those requiring probable cause continues a trend of Supreme Court jurisprudence dating back to at least *Katz* in 1967.[157]

vi. Riley v. California

Prior to *Carpenter*, the Supreme Court's most recent examination of the intersection of the Fourth Amendment and law enforcement surveillance was in 2014 in *Riley v. California*.[158] David Leon Riley brought a motion to suppress evidence after law enforcement warrantlessly searched his smartphone pursuant to his arrest.[159] The fruits from this search were

---

150. *See Jones*, 565 U.S. at 404.

151. *See* Peter C. Swire & William O'Neill, *A Reasonableness Approach to Searches After the* Jones *GPS Tracking Case*, 64 STAN. L. REV. ONLINE (2012), https://www.stanfordlawreview.org/online/privacy-paradox-a-reasonableness-approach-to-searches-after-the-jones-gps-tracking-case/ [https://perma.cc/RNX3-PH38].

152. *See id.*

153. *See id.*

154. *See Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).

155. *Id.* at 430 (Alito, J., concurring).

156. *See* Fernandes, *supra* note 19.

157. *See supra* Section I.B.i.

158. 573 U.S. 373 (2014).

159. *See id.* at 379.

later used against him in court.[160] *Riley* is significant because it set a bright-line rule that the Supreme Court will protect digital information stored *within* cell phones. The Court unanimously held that law enforcement generally needs a warrant to search a cell phone's digital contents, even where the search occurs during an otherwise lawful arrest.[161] The Court also held that when the Fourth Amendment is invoked, law enforcement must always procure a probable cause warrant.[162]

Chief Justice Roberts compared the Government's contention that a cell phone search is "materially indistinguishable" from tangible property searches to "saying a ride on horseback is materially indistinguishable from a flight to the moon . . . . Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[163] The Chief Justice provided the same instructions that were later repeated in *Carpenter*: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant."[164] The *Riley* Court emphasized the overarching privacy concerns of a warrantless law enforcement cell phone search.[165] Searching CSLI often reveals the most intimate details of a person's life, such as visits to medical clinics and trips to the liquor store.[166]

II. DAZED AND CONFUSED: HOW STATES AND LOWER COURTS ARE TREATING CSLI POST-*CARPENTER*

Section II.A discusses instances where state legislatures and lower courts have extended *Carpenter* to cover various warrantless law enforcement CSLI searches. Section II.B considers courts that have either denied extending *Carpenter* or ruled without reaching the question of warrantless real-time and shorter duration CSLI searches.

The *Carpenter* Supreme Court "decline[d] to say whether there is any sufficiently limited period of time 'for which the Government may obtain

---

160. *See id.* at 379–80

161. *See id.* at 403.

162. *See* Chaz Arnett, Carpenter *and the Future of the Surveillance State*, JURIST (July 17, 2019, 7:56 AM), https://www.jurist.org/commentary/2018/07/chaz-arnett-surveillance-carpenter/ [https://perma.cc/E3JV-UPHC].

163. *Riley*, 573 U.S. at 393.

164. *Id.* at 403; *see* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one — get a warrant.").

165. *See Riley*, 573 U.S. at 386.

166. *See* Arnett, *supra* note 162.

an individual's historical [CSLI] free from Fourth Amendment scrutiny.'"[167] The Court was worried about setting a clear rule that, over time, could seem obsolete. If "access to seven days' worth of information *does* trigger Fourth Amendment scrutiny," Gorsuch questioned, "[w]hy seven days instead of ten or three or one?"[168] Bright lines are oftentimes criticized as arbitrary. Indeed, the rule established in *Carpenter* is already causing confusion amongst lower courts.[169] Justice Gorsuch wrote that "[a]ll we know [from *Carpenter*] is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned."[170] The next Section illustrates how courts treat CSLI searches differently, an issue which Justice Gorsuch forewarned us about.

A. Legislatures and Courts Are Extending *Carpenter*

The following state supreme court and lower federal court decisions find that law enforcement CSLI searches require a probable cause warrant post-*Carpenter*. This movement continues a trend Justice William J. Brennan recognized over 40 years ago — that "more and more state courts are construing state constitutional counterparts of provisions of the Bill of Rights as guaranteeing citizens of their states even more protection than the federal provisions."[171] Justice Brennan argued that federalism "must necessarily be furthered significantly when state courts thrust themselves into a position of prominence in the struggle to protect the people of our nation from governmental intrusions on their freedoms."[172] Social movements can utilize federalism to provide even greater protection for individuals than the Constitution, which only provides a floor of minimum protections that states may build upon. While post-*Carpenter*, the Fourth Amendment requires a warrant to search one week or more of historical CSLI, the complication of cases below demonstrates how states are using federalism to similarly protect real-time CSLI and historical CSLI of less than one week.

---

167. *Carpenter*, 138 S. Ct. at 2266 (Gorsuch, J., dissenting) (quoting *Carpenter*, 138 S. Ct. at 2217 n.3).

168. NEIL GORSUCH, A REPUBLIC, IF YOU CAN KEEP IT 159–60 (2019).

169. *Cf. id.* at 159–61 (explaining that confusion could arise from obligating lower courts to use "two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition").

170. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

171. William Brennan, *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 495 (1977).

172. *Id.* at 503.

i. Supreme Court of Connecticut

In *Connecticut v. Brown*, the Supreme Court of Connecticut originally stayed defendant Terrance Brown's appeal pending the Supreme Court's *Carpenter* decision.[173] The facts in *Brown* concerned law enforcement's real-time CSLI search during an ATM theft investigation.[174] Law enforcement acted pursuant to three ex parte orders.[175] They first compelled the suspect's cellular carrier, T-Mobile, to disclose three months of historical telephone records.[176] The other two ex parte orders were prospective, or real time, and required T-Mobile to "ping" the suspect's cell phone every ten minutes during predetermined times when future thefts were likely to occur.[177] Law enforcement determined that Brown's location matched the general time and location of multiple burglaries after these cell phone pings.[178] During trial, Brown moved to suppress the location evidence that law enforcement discovered after searching his historical and real-time CSLI.[179]

The Supreme Court of Connecticut held that these ex parte orders, which were granted based on a "reasonable and articulable suspicion" rather than "probable cause," violated Brown's Fourth Amendment protection against unreasonable searches and seizures.[180] The court expanded on *Carpenter* by declaring that "the prospective CSLI yielded from the real time tracking of the defendant's cell phone — implicates important privacy interests that are traditionally the type protected by the [F]ourth [A]mendment."[181] The court treated real-time and historic CSLI similarly after failing to find a material difference between the legitimate privacy interests of historical CSLI, which the *Carpenter* Court held is protected by the Fourth Amendment, and real-time location monitoring.[182] "A person does not surrender all [F]ourth [A]mendment protection by venturing into the public sphere. To the contrary, what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[183] *Brown* is important because it makes a bright-line ruling about real-time CSLI searches. "It is one of

173. *See* Connecticut v. Brown, 202 A.3d 1003, 1006 (Conn. 2019).
174. *See id.* at 1007.
175. *See id.* at 1008.
176. *See id.*
177. *See id.*
178. *See id.* at 1008–09.
179. *See id.* at 1009.
180. *See id.* at 1006–07.
181. *Id.* at 1017.
182. *See id.*
183. *Id.* (internal quotations omitted).

the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[184] Rights not reserved for the federal government belong to the states pursuant to the Tenth Amendment.[185] This approach works best for experimenting with novel solutions to complicated issues.[186] Connecticut's protection of real-time CSLI provides a fitting example of a "states as laboratories" approach.[187] If Connecticut's citizens value this common law protection from warrantless location searches, it may become a model for other states and lower courts.

ii. Supreme Court of Massachusetts

The Supreme Court of Massachusetts extended *Carpenter*'s probable cause warrant requirement to real-time CSLI.[188] In *Commonwealth v. Almonor*,[189] law enforcement warrantlessly "pinged" a murder suspect's cell phone in real time and discovered that he was inside of his ex-girlfriend's home, where he was quickly arrested.[190] The Government argued against requiring a probable cause search warrant because "they don't collect the content of phone calls and text messages but rather operate like pen-registers and trap-and-traces, collecting the equivalent

---

184. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932).

185. *See* U.S. CONST. amend. X.

186. Bradley A. Blakeman, *States Are the Laboratories of Democracy*, HILL (May 7, 2020, 7:30 AM), https://thehill.com/opinion/judiciary/496524-states-are-the-laboratories-of-democracy [https://perma.cc/Z46H-SL5J].

187. *See* Edmund Andrews, *Steven Callander: How to Make States "Laboratories of Democracy,"* STAN. BUS. (May 19, 2015), https://www.gsb.stanford.edu/insights/steven-callander-how-make-states-laboratories-democracy [https://perma.cc/34S3-P43G].

188. *See* Kade Crockford, *Mass. High Court Requires Warrants for Stingray, GPS Phone Surveillance*, ACLU MASS. (Apr. 23, 2019), https://www.aclum.org/en/publications/mass-high-court-requires-warrants-stingray-gps-phone-surveillance [https://perma.cc/5HBH-XJNW].

189. 120 N.E.3d 1183 (Mass. 2019).

190. *See Almonor*, 120 N.E.3d at 1188; Jennifer Lynch, *Massachusetts Court Blocks Warrantless Access to Real-Time Cell Phone Location Data*, ELEC. FRONTIER FOUND. (Apr. 24, 2019), https://www.eff.org/deeplinks/2019/04/massachusetts-court-blocks-warrantless-access-real-time-cell-phone-location-data [https://perma.cc/GU3C-256U]; *see also* U.S. Const. amend. IV ("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 . . . .").

of header information."[191] The court disagreed, holding that this search infringed upon the individual's protection from unreasonable searches and seizures, even more so than the warrantless search of Carpenter.[192] The Supreme Court of Massachusetts ruled according to Article 14 of the Massachusetts Declaration of Rights, which states, "[e]very subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions."[193] Massachusetts' high court held that "society's [reasonable] expectation has been that law enforcement could not secretly and instantly identify a person's real-time physical location at will."[194] The court considered the reasonableness of this search and found that "[a]llowing law enforcement to immediately locate an individual whose whereabouts were previously unknown by compelling that individual's cell phone to reveal its location contravenes that expectation."[195] The court's holding illustrates that both Massachusetts's Article 14 and "the longstanding protections of the Fourth Amendment apply with undiminished force to cell phone location records."[196] Massachusetts law now states that "[a] warrant is required to obtain a suspect's historical cell phone location information. An 'order issued under § 2703(d) of the [Stored Communications] Act, [18 U.S.C. § 2703(d)] is not a permissible mechanism for accessing historical cell-site records.'"[197] This case and Massachusetts' legislative acts illustrate how states can use their constitutions to protect their citizens from unreasonable searches and seizures beyond the federal minimum.[198]

---

191. Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, WIRED (Mar. 3, 2014, 9:00 AM), https://www.wired.com/2014/03/stingray/ [https://perma.cc/RV`6L-QXT8].

192. *See Almonor*, 120 N.E.3d at 1194 ("Manipulating our phones for the purpose of identifying and tracking our personal location presents an even greater intrusion [than *Carpenter*].").

193. MASS. CONST. Pt. 1, art. XIV.

194. *Almonor*, 120 N.E.3d at 1195.

195. *Id.*

196. Commonwealth v. Almonor, ACLU MASS., https://www.aclum.org/en/cases/commonwealth-v-almonor [https://perma.cc/ED4F-LJZ9] (last visited Aug. 18, 2020).

197. *Massachusetts Law About Cell Phone Searches*, MASS.GOV (Feb. 21, 2020) (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018)), https://www.mass.gov/info-details/massachusetts-law-about-cell-phone-searches [https://perma.cc/TVR7-YF7W].

198. *See generally* JEFFREY S. SUTTON, 51 IMPERFECT SOLUTIONS: STATES AND THE MAKING OF AMERICAN CONSTITUTIONAL LAW (2008) (discussing the importance of state constitutions as bulwarks against state abuse and the source of protections of individual rights).

iii. Maine Supreme Judicial Court

In *Maine v. O'Donnell*, the Maine Supreme Judicial Court stayed the appeal pending the Supreme Court's *Carpenter* decision.[199] At issue was whether law enforcement's warrantless real-time CSLI search was considered reasonable.[200] Law enforcement compelled Verizon, O'Donnell's service provider, to provide the real-time location of his and his girlfriend's cell phones.[201] Law enforcement submitted an "emergency disclosure form" to Verizon compelling such disclosure because the suspects were considered a flight risk.[202] Both individuals were quickly apprehended, and the stolen goods recovered. [203]

O'Donnell filed a motion to suppress his CSLI, citing both the Fourth Amendment and Maine's Electronic Device Location Information Act.[204] The court held that O'Donnell lacked standing to raise a Fourth Amendment defense because his location was ascertained using his girlfriend's CSLI: "[I]t is well-established that Fourth Amendment rights cannot be asserted vicariously."[205] O'Donnell's girlfriend chose to serve as an informant and permitted the warrantless search.[206] *O'Donnell* shows a state statute providing its citizens with broader freedom from unreasonable searches than what the U.S. Constitution permits. Maine requires warrants for both real-time and historical CSLI searches under its Electronic Device Location Information Act except during exigent circumstances.[207] Maine is 1 of 18 states that currently have some warrant requirement for CSLI searches.[208]

---

199. *See* Maine v. O'Donnell, 210 A.3d 815, 819 (Me. 2019); *see also ACLU Weighs in on Maine Cell Phone Tracking Case Following U.S. Supreme Court Victory*, ACLU (Aug. 30, 2018) [hereinafter *ACLU Weighs In*], https://www.aclu.org/press-releases/aclu-weighs-maine-cell-phone-tracking-case-following-us-supreme-court-victory [https://perma.cc/9JXT-XU2Y].

200. *See O'Donnell*, 210 A.3d at 817.

201. *See id.* at 818.

202. *See id.*

203. *See id.* at 819.

204. *See id.* at 820; *ACLU Weighs In*, *supra* note 199.

205. *O'Donnell*, 210 A.3d at 820–21 (quoting Rakas v. Illinois, 439 U.S. 128, 133–34 (1978)).

206. *See id.* at 820.

207. *See* ME. STAT. tit. 16 §§ 648, 650(4) (2019); Brief for American Civil Liberties Union of Maine et al. as Amici Curiae Supporting Appellant at 36, Maine v. O'Donnell, 210 A.3d 815 (Me. 2019) (No. Fra-17-12).

208. Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, ACLU (Aug. 26, 2015), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015 [https://perma.cc/ZL5P-JW9M]. These states are California, Colorado, Florida, Illinois, Indiana, Iowa, Maine, Maryland, Massachusetts, Minnesota, Montana, New Hampshire, New Jersey, Tennessee, Utah, Virginia, Washington, and Wisconsin. *See id.*

iv. New York County Supreme Court

The New York County Supreme Court heard a motion to vacate a conviction based on real-time and historical CSLI post-*Carpenter* in *People v. Cutts*.[209] Aljulah Cutts argued that his conviction relied upon CSLI and should be retroactively overturned post-*Carpenter*.[210] The court order law enforcement obtained was supported by probable cause.[211] This order authorized "the installation and use of a pen register and a trap device, including caller identification and cell site information, and indicated that '[p]robable cause has been established to show that GPS/precision location is relevant to an ongoing criminal investigation.'"[212] New York's probable cause requirement for location information exemplifies federalism in action by going beyond the Fourth Amendment's minimum safeguards.[213]

New York's heightened probable cause requirement demands a higher showing from law enforcement than the federal SCA's "reasonable grounds to believe" threshold. States are free to "apply state constitutional provisions [that are] more protective of freedom than their federal counterparts."[214] In other words, they may require a probable cause showing for real-time CSLI searches, even where the federal protections are less. States need not "stay tuned"[215] for the United States Supreme Court to expand on *Carpenter* before providing their citizens with additional protection from unreasonable searches.

v. Queens County Supreme Court

In *People v. Simpson*,[216] New York's Queens County Supreme Court had to apply *Carpenter* during an ongoing trial because the decision came out just two days after historical CSLI was admitted into evidence.[217] This court had held, prior to *Carpenter*, that "an individual does not have a legitimate expectation of privacy in his/her CSLI."[218] The Government in *Simpson* presented an expert witness from T-Mobile to testify that

---

209. 88 N.Y.S.3d 332 (Sup. Ct. 2018).

210. *See id.* at 334.

211. *See id.* at 335.

212. *Id.* at 335–36.

213. *See, e.g.*, *In re Dist. Att'y v. Angelo G.*, 371 N.Y.S.2d 127 (App. Div. 1975).

214. *State Constitutions: Freedom's Frontier*, CATO POL'Y REP. 9, 9 (Nov.–Dec. 2016), https://www.cato.org/sites/cato.org/files/serials/files/policy-report/2016/12/cpr-v38n6-4.pdf [https://perma.cc/3Q66-87ZZ].

215. Carpenter v. United States, 138 S. Ct. 2206, 2267 (2018) (Gorsuch, J., dissenting).

216. 88 N.Y.S.3d 763 (Sup. Ct. 2018).

217. *See id.* at 766.

218. *Id.* at 773–74.

Maurice Simpson's phone "pinged" a cell tower within minutes of a nearby robbery, and that Simpson's historical CSLI suggested that he was not ordinarily in that area.[219] *Carpenter* forced the court to revisit its previous decision to admit the defendant's historical CSLI into evidence.[220] The court explained that in New York, "[f]undamental to the issuance of any search warrant is a finding by a neutral and detached magistrate that probable cause exists."[221]

Simpson underscores the confusion that lower courts will continue to face until the Supreme Court makes definitive rulings over different warrantless CSLI searches. In this case, only three days of historical CSLI was admitted into evidence.[222] The Supreme Court in *Carpenter* only definitively held that searching seven days or more of historical CSLI requires a probable cause warrant.[223] Thus, the Government argued that *Carpenter* is inapplicable to searches of less than seven days.[224] This argument is inconsistent with *Carpenter*, however, as the Supreme Court expressly left that issue unanswered:

> [W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient . . . to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.[225]

Until a definitive federal action is taken, future courts will continue to have to rule on whether accessing less than seven days of historical CSLI requires a warrant under the Constitution— either the Supreme Court takes on a CSLI case and clarifies, or the legislature passes legislation recognizing CSLI as property.[226]

vi. States Are Acting Independently to Add to Carpenter

The above cases show state legislatures implementing safeguards to protect individual location records held by third-party service providers. Furthermore, they show state courts expanding traditional Fourth

---

219. *See id.* at 770.
220. *See id.* at 771.
221. *Id.*
222. *Id.* at 766.
223. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
224. *Simpson*, N.Y.S.3d at 767.
225. *Carpenter*, 138 S. Ct. at 2217 n.3.
226. *See* Megan Graham, *The Fourth Amendment and Third Party Doctrine After* Carpenter 10 (Feb. 2, 2019), https://nj.fd.org/sites/nj.fd.org/files/cja-seminar-materials/2019/Post-Carpenter-Litigation-Outline.pdf [https://perma.cc/T4WD-CHJY].

Amendment protection by requiring a warrant for real-time CSLI collection. Justice Gorsuch remarked that the Fourth Amendment means more than "protecting only the specific rights known at the founding; it means protecting their modern analogues too."[227] An individual's CSLI held by third parties may, in fact, enjoy the same protection as traditionally protected categories. "[I]f state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations."[228] Put another way, states may order that obtaining real-time CSLI also requires a warrant, notwithstanding *Katz*'s reasonable expectation of privacy test and the Third Party Doctrine. As Justice Gorsuch analogized, "[w]hatever may be left of [the Third Party Doctrine], few doubt that e-mail should be treated much like the traditional mail it has largely supplanted."[229] State legislatures and courts have largely forbidden warrantless searches of an individual's real-time location.[230] In so doing, they made a laudable societal judgment that the expectation of privacy over CSLI requires a warrant. This is a decision that the federal government is still unprepared to take.

B. Supreme Deference: Lower Courts Avoiding or Declining to Extend *Carpenter*

The cases below represent how other courts are limiting or otherwise avoiding warrantless real-time CSLI searches post-*Carpenter*. This judicial response can be attributed to (1) *Carpenter*'s narrow applicability and silence regarding real-time CSLI and (2) societal expectations regarding when warrantless law enforcement CSLI searches are appropriate under the Fourth Amendment's "reasonableness" standard.

i. United States District Court for the District of Massachusetts

In *United States v. Saemisch*, the United States District Court for the District of Massachusetts declared that "if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI."[231] The court noted *Carpenter*'s silence

227. GORSUCH, *supra* note 168, at 164.

228. *Id.*

229. *Id.* at 163.

230. *See generally supra* Section II.A.

231. United States v. Saemsich, 371 F. Supp. 3d 37, 42 (D. Mass. 2019) (quoting Kentucky v. King, 563 U.S. 452, 460 (2011)).

regarding the constitutionality of real-time CSLI searches,[232] but reiterated the Court's stance that "even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances."[233] One such exception occurs when law enforcement face an exigent circumstance.[234]

In this case, an informant alerted law enforcement that Christopher Saemisch had access to children and planned to have "sexual relationships" with them.[235] An undercover investigation led to Saemisch, confirming his plans.[236] However, when law enforcement arrived at his home the next day, Saemish was gone.[237] Homeland Security located Saemisch by ordering AT&T to warrantlessly "ping" his cell phone.[238] The SCA permits service providers to divulge CSLI to government agencies without an order where it "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay."[239] The court found this warrantless search to be reasonable because "there were exigent circumstances that supported an objectively reasonable belief that the defendant posed a potentially imminent threat to the safety of identified minor children."[240] The Massachusetts federal court ruled on the Fourth Amendment's exigent circumstances exception[241] instead of more broadly addressing the constitutionality of warrantless real-time CSLI searches post-*Carpenter*.[242] *Saemisch* illustrates how warrantless real-time CSLI searches can provide a communal benefit by giving law enforcement the capability to mitigate an exigent threat quickly. The Fourth Amendment's exigent circumstances exception balances the individual's right to be free from unreasonable searches and seizures on the one hand, and critical law enforcement and national security needs on the other.[243]

---

232. *See id.* at 42.
233. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).
234. *See Saemisch*, 371 F. Supp. 3d at 42.
235. *See id.* at 39.
236. *See id.* at 40.
237. *See id.*
238. *See id.*
239. 18 U.S.C. § 2702(c)(4); *see also Saemisch*, 371 F. Supp. 3d at 40.
240. *Saemisch*, 371 F. Supp. 3d at 42.
241. *See id.*
242. *See id.*
243. Michelle Perin, *Technology after* Carpenter, OFFICER.COM (Sept. 17, 2018), https://www.officer.com/command-hq/technology/article/21017662/what-does-carpenter-mean-for-law-enforcement [https://perma.cc/5QJ5-2NSN].

ii. Supreme Court of Florida

The Supreme Court of Florida, Florida's highest court, found *Carpenter* inapplicable where law enforcement searched an individual's real-time location with a portable "cell-site simulator."[244] A cell-site simulator, also known as "Sting Ray" or "IMSI Catcher," is a moveable device originally designed for military and intelligence communities that "simulates a cellphone tower in order to trick nearby mobile devices into connecting to it and revealing their location."[245] Its portability allows the government to triangulate a suspect's location with much greater accuracy than the fixed cell towers searched in *Carpenter*.[246] This technology is controversial today because it "collaterally gather[s] data from innocent bystanders' phones and can interrupt phone users' service — which critics say violates a federal communications law."[247] Nevertheless, law enforcement agencies use cell-site simulators throughout the country in unknown numbers.[248]

In *Andres v. State*, law enforcement used a cell-site simulator to execute a probable cause warrant.[249] The warrant covered Rafael Andres's DNA and photographs of his body, but not his physical location.[250] The court denied Andres's motion to suppress the CSLI evidence acquired from the cell-site simulator because law enforcement procured a valid warrant in good faith.[251] The court also declined to extend *Carpenter*'s warrant requirement to real-time CSLI:

> We take notice of the United States Supreme Court's recently issued decision in *Carpenter v. United States* . . . . However, we conclude that its holding is not applicable to this case, where officers used real-time cell-site location information to locate Andres for the purposes of executing the warrant.[252]

---

244. Andres v. State, 254 So. 3d 283, 298 n.7 (Fla. 2018).

245. Zetter, *supra* note 191.

246. *Id.*

247. Ryan Gallagher, *FBI Documents Shine Light on Clandestine Cellphone Tracking Tool*, SLATE (Jan. 10, 2013, 2:14 PM), https://slate.com/technology/2013/01/stingray-imsi-catcher-fbi-documents-shine-light-on-controversial-cellphone-tracking-tool.html [https://perma.cc/X97F-LHTV]; *see also* Yomna Nasser, *Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, ELEC. FRONTIER FOUND. (June 28, 2019), https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks [https://perma.cc/FRR9-DWSQ].

248. Gallagher, *supra* note 247.

249. *Andres*, 254 So. 3d, at 298.

250. *See id.*

251. *See id.*

252. *Id.* at 297 n.7.

Andres emphasized *Carpenter*'s narrow applicability.[253] The Supreme Court of Florida recognized that *Carpenter* only definitively ruled on historical CSLI searches and declined to extend such warrant protection to real-time CSLI searches.[254] This illustrates a measure of judicial restraint, which harkens back to the Warren Supreme Court's push in "both deferring to the people and allowing Congress wide latitude to pass legislation that best protected [people in the United States'] rights."[255] The Warren Court believed that "[b]y definition repeat losers in the majoritarian political process, discrete and insular minorities only achieve victories in that process with intense effort and years of activism. Their successful struggle to obtain legislation that protects their rights deserves respect from the courts in the form of deference to that legislation."[256] Judges may be ill-equipped to make societal decisions intended for the legislature. "Politically insulated judges come armed with only the attorney's briefs, a few law clerks, and their own idiosyncratic experiences. They are hardly the representative group you'd expect (or want) to be making empirical judgments for hundreds of millions of people" because they often "fail to reflect public views."[257] The Supreme Court of Florida's nonfeasance here gives deference to state and federal legislative enactments, as well as respect for the governmental separation of powers, because the legislature represents the people's perspectives about reasonable warrantless searches.

iii. Court of Appeals of Indiana

Indiana's intermediate Court of Appeals permitted a real-time CSLI search under the Fourth Amendment's exigent circumstances exception in *Govan v. State of Indiana*.[258] Here, law enforcement interviewed a woman, seriously injured allegedly by Morgan Govan, in a hospital.[259] The victim's mother provided investigators with Govan's cell phone number.[260] Obtaining the phone number allowed law enforcement to contact Sprint, the suspect's service provider, and ask them to provide

253. *See id.*

254. *See id.*

255. Sandhya Bathija, *Why Judicial Restraint Best Protects Our Rights*, CATO UNBOUND (Feb. 7, 2014), https://www.cato-unbound.org/2014/02/07/sandhya-bathija/why-judicial-restraint-best-protects-our-rights#_ftnref5 [https://perma.cc/B4XS-LGDZ].

256. Rebecca A. Zietlow, *The Judicial Restraint of the Warren Court (and Why it Matters)*, OHIO ST. L.J. 255, 260 (2007).

257. GORSUCH, *supra* note 168, at 157.

258. 116 N.E.3d 1165 (Ind. Ct. App. 2019).

259. *See id.* at 1169.

260. *See id.*

"emergency or exigent ping[s]" to ascertain Govan's real-time CSLI.[261] Law enforcement's supporting affidavit to Sprint stated that Govan "restrain[ed] [two women] in his basement and brutally beat[] them for forty-five minutes," that one victim's mother provided Govan's phone number to investigators at the hospital, and that "Govan knew where they lived . . . [and] had tried to contact [the victims] via Facebook . . . at the hospital."[262] Sprint complied, and law enforcement apprehended the defendant within two hours.[263] Govan later filed a motion to suppress this real-time CSLI evidence under both the Indiana and federal constitutions.[264]

The court noted that *Carpenter* declined to rule on the constitutionality of warrantless real-time CSLI searches,[265] but ruled that law enforcement's "need to assist persons who are seriously injured or threatened with such injury" met the Fourth Amendment's exigent circumstance exception.[266] Additionally, this service provider's internal procedures also provided a secondary layer of protection from arbitrary warrantless searches: "Sprint makes an independent determination about whether the situation is exigent and does not merely rubber-stamp a police officer's request."[267] The court of appeals affirmed the trial court's denial of Govan's motion to suppress the warrantless real-time CSLI search.[268] This case provides another example of an instance where law enforcement can warrantlessly search real-time CSLI under the Fourth Amendment's exigent circumstance exception, regardless of *Carpenter*'s narrow applicability.[269]

The Supreme Court has set forth instances where exigent circumstances make warrantless searches objectively reasonable under the Fourth Amendment.[270] Such instances include officers providing emergency aid[271] and hot pursuit of a fleeing suspect.[272] Courts have held

261. *Id.* at 1170.
262. *Id.* at 1173.
263. *See id.* at 1170.
264. *See id.*
265. *See id.* at 1172.
266. *Id.* (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).
267. *Id.* at 1173.
268. *See id.* at 1178.
269. *See id.* at 1172.
270. *See* Kentucky v. King, 563 U.S. 452, 460 (2011).
271. *See Brigham City*, 547 U.S. at 403.
272. *See* United States v. Santana, 427 U.S. 38, 42–43 (1976).

that when such situations arise, society has "objectively" determined that warrantless searches are reasonable during an emergency.[273]

The various approaches from lower courts on warrantless CSLI searches indicate that an individual's protection against such searches depends largely upon which state they are being investigated in. *Carpenter*'s equivocal treatment of real-time CSLI furthers this dilemma. Lower courts lack the power to seriously call into question the Third Party Doctrine and *Katz*'s reasonable expectation of privacy test as it relates to warrantless searches of an individual's location.[274] On the other hand, the Supreme Court can extend *Carpenter*'s national protection to both real-time CSLI searches and historical CSLI searches of less than seven days.[275] In doing so, the Court can ensure that every person in the United States is protected against unreasonable warrantless location searches. Today, only some people in the United States enjoy this right. Resolving questions post-*Carpenter*, like which warrantless CSLI searches comport with the Fourth Amendment, must balance society's expectation about reasonable warrantless searches and the need for efficient law enforcement investigations. What follows are possible solutions that may be taken to address *Carpenter*'s ambiguity.

III. PROGRESSIVE FEDERALISM: IMPLEMENTING JUSTICE GORSUCH'S PROPERTY-BASED APPROACH TO PROTECT ALL CSLI

Justice Breyer remarked that warrantless CSLI searches are "an open box. We know not where we go."[276] This Section reviews how the *Carpenter* Court's majority and dissents may address real-time CSLI searches and CSLI searches of less than seven days. Part III concludes by advocating for Justice Gorsuch's property-based approach to protect all CSLI at the federal level and encourages states to safeguard their own citizens' rights in the meantime. Part II exemplified how *Carpenter*'s narrow holding falls short in rectifying the existing gap between (1) historical CSLI searches of one week or more that require a warrant post-*Carpenter*, and (2) real-time CSLI searches and historical CSLI

273. *See, e.g.*, *Brigham City*, 547 U.S. at 400 (holding that the emergency-aid exception to the warrant requirement allows warrantless home searches where police have an "objectively reasonable basis for believing that an occupant is seriously injured or imminently threatened with such injury"); *see also* Wyoming v. Houghton, 526 U.S. 295, 299–300 (1999) (discussing the balancing act between the government interest, as represented by society, and the individual right to privacy when determining exceptions to the Fourth Amendment).

274. *See* GORSUCH, *supra* note 168, at 165.

275. *See id.*

276. Transcript of Oral Argument, *supra* note 38, at 34.

searches of less than one week, which the *Carpenter* court declined to rule on. There is currently a judicial split over whether this second category requires a warrant.

Furthermore, the Supreme Court is divided over whether other warrantless CSLI searches should be governed under *Katz*'s "reasonable expectation of privacy test, the Third Party Doctrine's reasonable grounds to believe standard, or as "property" under the Fourth Amendment. For this reason, state legislatures and courts should adopt the measures taken by states like Connecticut, Massachusetts, Maine, and New York to protect all of their citizens' CSLI. A movement like this can influence the Supreme Court, which has historically changed positions based upon societal trends and changes in state laws.[277]

A. The *Katz* Is Out of the Bag: Judges Are Ill-Equipped to Measure Societal Expectations of Privacy

The *Carpenter* majority found that law enforcement's warrantless CSLI search violated Carpenter's "legitimate expectation of privacy in the record of his physical movements" under *Katz*.[278] The Court recognized that individuals "compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[279] Accordingly, it extended traditional Fourth Amendment property protection to Carpenter's CSLI.[280] As a result, law enforcement needs a warrant to search historical CSLI of one week or more. It remains to be seen how the Court will treat warrantless real-time CSLI searches and historical CSLI searches lasting less than one week, however.[281]

---

277. *Judicial Decision-Making and Implementation by the Supreme Court*, ST. UNIV. N.Y., https://courses.lumenlearning.com/suny-amgovernment/chapter/judicial-decision-making-and-implementation-by-the-supreme-court/ [https://perma.cc/X6A2-C5PP] ("In the 1960s, sodomy was banned in all the states. By 1986, that number had been reduced by about half. By 2002, thirty-six states had repealed their sodomy laws, and most states were only selectively enforcing them. Changes in state laws, along with an emerging LGBT movement, no doubt swayed the Court and led it to the reversal of its earlier ruling with the 2003 decision, *Lawrence v. Texas*.").

278. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

279. *Id.* at 2218.

280. *See id.*

281. *See id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records

According to Justice Gorsuch, *Katz*'s reasonable expectation of privacy test is inconsistent with both the Constitution's text and intent because it shoehorned "privacy" into the Fourth Amendment.[282] Justice Gorsuch stated that "[t]he framers chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things — 'persons, houses, papers, and effects' — and against particular threats — 'unreasonable' governmental 'searches and seizures.'"[283] *Katz*'s reasonable expectation of privacy standard has replaced the framers' objective thoughts on unreasonable searches with judicial discretion and flexibility.[284] However, such "judicial judgments often fail to reflect public views."[285] Indeed, the judiciary is "hardly the representative group you'd expect (or want) to be making empirical [or normative] judgments for hundreds of millions of people."[286] That is a role best left up to Congress. Thus, Justice Gorsuch argues that *Katz*'s ongoing problem is that it substitutes the legislature's majoritarian perspective on reasonable warrantless law enforcement searches with a judge's so-called subjective "judicial imagination."[287]

B. Big Brother Is Watching: The Third Party Doctrine Gives Law Enforcement Carte Blanche to Warrantlessly Search an Individual's Location

In *Carpenter*, Justice Kennedy, joined by Justices Thomas and Alito, dissented on the grounds that CSLI should be treated as an ordinary business record under the Third Party Doctrine.[288] The Third Party Doctrine is an extension of *Katz*'s reasonable expectation of privacy test,[289] and would permit real warrantless real-time CSLI searches and searches of less than a week because there is no protection in CSLI controlled by service providers.[290] In other words, turning over business

---

that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").

282. *See* GORSUCH, *supra* note 168, at 157; *supra* Sections I.A.iii.b–d.

283. *See* GORSUCH, *supra* note 168, at 157.

284. *See id.*

285. *Id.*

286. *Id.*

287. *Id.* at 156; *supra* Section I.A.ii.1.

288. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (Kennedy, J., dissenting).

289. *See* GORSUCH, *supra* note 168, at 156.

290. *See id.*

> Another justification sometimes offered for third party doctrine is clarity. You (and the police) know exactly how much protection you have in information confided to others: none. As rules go, "the king always wins" is admirably clear.

records to a third party negates any "expectation of privacy" in those records.[291] One benefit from this bright-line rule is that the judiciary defers to the democratically accountable legislature when deciding what society would deem reasonable under the Fourth Amendment.[292] Congress is in a better position to gauge societal reasonableness as democratically-elected public servants.[293] Thus, the SCA's Section 2703(d) order, which requires "reasonable grounds to believe" instead of "probable cause," would constitutionally permit warrantless real-time CSLI searches and searches of less than a week under the Third Party Doctrine.

The Supreme Court established the Third Party Doctrine long before society's "seismic shift" into the digital age.[294] This is why today, most legal commentators believe "the Third Party Doctrine is not only wrong, but horribly wrong."[295] Warrantless digital location surveillance is markedly different from the bank records and phone numbers that the Supreme Court permitted law enforcement to warrantlessly search in *Smith* and *Miller*.[296] "It is a Fourth Amendment fiction that individuals 'voluntarily' convey CSLI [pursuant to the Third Party Doctrine] as one would dial a phone number. Users do not intentionally create CSLI and have no real choice in the matter."[297] Still, under the Third Party Doctrine, the 95% of cell phone owners risk law enforcement warrantlessly searching their location under a lower standard than the Fourth Amendment requires.[298] Adding to this problem is that many Americans are unaware that service providers even collect and store their

---

> But the opposite rule would be clear too: Third party disclosures *never* diminish Fourth Amendment protection (call it "the king always loses").

Id.

291. *See supra* Section I.B.ii.

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

293. *See id.*

294. *See id.* at 2219.

295. Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009); *see also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(C) (5th ed. 2019) ("The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection the Court had developed in *Katz*.").

296. *See supra* Section I.B.ii.

297. Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Petitioner at 20–21, Carpenter v. United States., 138 S. Ct. 2206 (2018) (No. 16-402).

298. *See Carpenter*, 138 S. Ct. at 2211 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."); *see also ACLU Weighs In*, *supra* note 199.

every movement.[299] So "[i]n the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."[300]

Both *Katz* and the Third Party Doctrine are suboptimal approaches to resolve warrantless CSLI searches post-*Carpenter*. These approaches fail to resolve the profoundly impactful issues surrounding warrantless police searches of an individual's real-time CSLI and CSLI of less than seven days. The Fourth Amendment's protection against unreasonable searches and seizures demands more than that.[301] But there is another option.

C. Throw the Baby Out with the Bathwater: Protect CSLI through Fourth Amendment "Property" Categorization

The Fourth Amendment protects people from unreasonable warrantless law enforcement searches regardless of the era they live in. Although the Framers had no concept of CSLI in 1789, they internalized an innate appreciation of property rights in early America from English common law.[302] In *Entick v. Carrington*,[303] for example, England's King's Bench created significant restrictions on the scope of executive power.[304] This judicial check on governmental authority was highly praised in America and inspired the Fourth Amendment.[305] In *Entick*, a case widely recognized as "a heralded decision that the founding generation considered 'the true and ultimate expression of constitutional law,' . . . Lord Camden explained that '[t]he great end, for which men entered into society, was to secure their property.'"[306] This property-based approach to unreasonable searches may be extended to CSLI and thus better protects against warrantless CSLI searches than *Carpenter*, *Katz*, and the Third Party Doctrine.

---

299. *See* Rob Pegoraro, *Apple and Google Remind You About Location Privacy, but Don't Forget Your Wireless Carrier*, USA TODAY (Nov. 23, 2019, 6:00 AM), https://www.usatoday.com/story/tech/columnist/2019/11/23/location-data-how-much-do-wireless-carriers-keep/4257759002/ [https://perma.cc/ANC2-8Z6Z].

300. *See* GORSUCH, *supra* note 168, at 156.

301. *See id.* at 153.

302. *See Carpenter*, 138 S. Ct. at 2239 (Thomas, J., dissenting); *see also* United States v. Di Re, 332 U.S. 581, 595 (1948) (noting that the Framers' priority regarding the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance").

303. 19 How. St. Tr. 1029 (K.B. 1765).

304. *See* Robert J. Reinstein, *The Limits of Executive* Power, 59 AM. U. L. REV. 259, 283 (2009).

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

306. *Id.* (quoting Boyd v. United States, 116 U.S. 616, 626 (1886)).

Indeed, Justice Gorsuch's *Carpenter* dissent urged future defendants to employ this property-based argument the next time law enforcement warrantlessly searches an individual's digital location.[307] This defense classifies third-party service providers as "bailees"[308] who owe a legal duty to the individual to secure their location information.[309] Justice Gorsuch made the apt comparison: "Ever . . . [a]sk your neighbor to look after your dog while you travel? You would not expect . . . the neighbor to put Fido up for adoption."[310] It is important to note that CSLI is not wholly analogous to a dog, but, in any case, recent Supreme Court decisions have implied that "the use of technology is functionally compelled by the demands of modern life, and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too."[311] It is high time for the federal government to recognize that its decisions from the 1970s and telecommunication regulations from the 1980s are ill-equipped to govern warrantless law enforcement CSLI searches in 2020. States and lower courts can provide the catalyst for this societal change in much the same way that the LGBT movement influenced the Supreme Court in *Lawrence v. Texas*, a monumental decision that made anti-sodomy laws unconstitutional throughout America.[312] Classifying CSLI as property under the Fourth Amendment would best protect individuals from warrantless historical and real-time CSLI searches.

CONCLUSION

Carpenter took the next step of preventing seemingly Orwellian levels of warrantless law enforcement surveillance, but the battle for digital privacy rages on.[313] Legal commentators Albert Fox Cahn and Karin

---

307. *See id.* at 2272 (Gorsuch, J., dissenting) ("Litigants have had fair notice since at least *United States v. Jones* (2012) and *Florida v. Jardines* (2013) that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not. Yet the arguments have gone unmade, leaving courts to the usual *Katz* handwaving. These omissions do not serve the development of a sound or fully protective Fourth Amendment jurisprudence.").

308. *Id.* at 2268.

309. *An Introduction to Bailee Liability Concepts*, INLAND MARINE UNDERWRITERS ASS'N: BAILEES & PROCESSORS COMM. (1994), https://www.imua.org/Files/reports/An%20Introduction%20to%20Bailee%20Liability%20Concepts.html [https://perma.cc/39CB-CASG].

310. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

311. *See* GORSUCH, *supra* note 168, at 163.

312. *See Judicial Decision-Making and Implementation by the Supreme Court*, *supra* note 277.

313. Albert Fox Cahn & Karin Bashir, Carpenter *Ruling Brings Us Back from Brink of Orwellian Surveillance State*, JUST SEC. (June 28, 2018),

Bashir note that "[a]s the law struggles to keep pace with the growth of cheap, powerful, and prolific tracking tools, *Carpenter* marks a crucial step away from formalistic privacy analysis that hobbled prior Fourth Amendment cases."[314] Currently, *Carpenter*'s equivocal position on real-time CSLI searches and historical CSLI searches of less than seven days inhibits lower courts from providing congruent holdings as to the constitutionality of warrantless CSLI searches. Federally, all that the Supreme Court made certain post-*Carpenter* is that searching seven or more days of CSLI requires a warrant.[315] As for everything else, America must "stay tuned."[316] The judiciary and legislature should clearly demarcate which warrantless CSLI searches infringe upon the individual's Fourth Amendment freedom from unreasonable searches and seizures. As stated by the Electronic Frontier Foundation, "[o]ne key way courts put this into practice is by creating bright-line rules that signal to the police and citizens alike what is covered by the warrant requirement."[317]

The Supreme Court and Congress's nonfeasance today should also motivate states to develop their own safeguards against warrantless CSLI searches. Thomas Jefferson once stated that "free people claim[] their rights, as derived from the laws of nature, and not as the gift of their chief magistrate."[318] Stanford Professor Steven Callander posits that implementing a "states as laboratories" approach to CSLI laws exemplifies

> "progressive federalism," in which the national government orchestrates a "sort-of tournament" between states to find the best solution to a problem. The state that comes up with the "winning' approach" — the policy showing the best outcomes — gets to keep it, while the other states must adopt that winning policy . . . .[319]

Even post-*Carpenter*, states can act independently to require a warrant for all law enforcement CSLI searches. A number of states are actively working to classify various digital and electronic mediums as

---

https://www.justsecurity.org/58607/carpenter-ruling-brings-brink-orwellian-surveillance-state/ [https://perma.cc/64T9-9B2L].

314. *Id.*

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

316. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

317. Andrew Crocker, *Massachusetts Court Rules Cell Tracking Requires a Warrant*, ELEC. FRONTIER FOUND. (Sept. 28, 2015), https://www.eff.org/deeplinks/2015/09/massachusetts-court-rules-cell-tracking-requires-warrant [https://perma.cc/7X2F-RXWH].

318. THOMAS JEFFERSON, A SUMMARY VIEW OF THE RIGHTS OF BRITISH AMERICA 22 (1774).

319. Andrews, *supra* note 187.

"property."[320] Should this trend continue, the "winning" approach may become the next defense against warrantless CSLI searches.

320. *See, e.g.*, TEX. PROP. CODE ANN. § 111.004(12) (West 2017) (defining "property" to include "property held in any digital or electronic medium"); Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 768 (2017) (e-mail account is a "form of property often referred to as a 'digital asset'"); Eysoldt v. ProScan Imaging, 957 N.E.2d 780, 786 (2011) (permitting action for conversion of web account as "intangible property").