Loyola of Los Angeles Law Review

Volume 53 | Number 3 Article 5

Spring 5-1-2020

Cell-Site Location Information and the Privacies of Life: The Impact of Carpenter v. United States

Trevor Moore

CELL-SITE LOCATION INFORMATION AND THE PRIVACIES OF LIFE: THE IMPACT OF *CARPENTER V. UNITED STATES*

*Trevor Moore**

I. INTRODUCTION

Cell phones have become an "important feature of human anatomy,"[1] and Americans should not forfeit their Fourth Amendment rights simply for owning one. The Framers' central aim in drafting the Fourth Amendment, as the Supreme Court has made clear, was to secure "'*the privacies of life*' against 'arbitrary power,'"[2] which includes placing "obstacles in the way of a too permeating police surveillance."[3] However, as technology has advanced, Fourth Amendment protections have become weaker and weaker.

For example, law enforcement may now use cell phones and cell-site location information (CSLI) to discover an individual's location.[4] Prior to June 22, 2018, law enforcement could contact a cell phone service provider, such as Verizon, T-Mobile, or Sprint, and obtain CSLI by demonstrating to a judge that the "records sought '[were] relevant and material to an ongoing criminal investigation.'"[5] This standard is extremely easy to meet and "falls well short of the probable cause required for a warrant."[6]

This type of surveillance is "too permeating,"[7] and without change, Americans will be left "at the mercy of advancing

* J.D. Candidate, May 2020, Loyola Law School, Los Angeles; B.A., Criminal Justice, California State University, Chico, May 2012. Thank you to the editors and staff of the *Loyola of Los Angeles Law Review* for their hard work in editing this Note. In addition, thank you to my family for the constant love and support.

1. Riley v. California, 573 U.S. 373, 385 (2014).
2. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (emphasis added) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
3. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
4. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner at 16, Rios v. United States, 138 S. Ct. 2701 (2018) (No. 16-7314).
5. *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d) (2012)).
6. *Id.* at 2221.
7. *Id.* at 2214 (quoting *Di Re*, 332 U.S. at 595).

technology."[8] Fortunately, in *Carpenter v. United States*,[9] the Supreme Court made the requirements to obtain CSLI more stringent.[10] However, while this modification was a big step in the right direction, it was not enough.

This Note explains the impact *Carpenter* had on determining whether individuals maintain a legitimate expectation of privacy in the records of their physical movements captured through real-time CSLI. Further, this Note proposes that real-time CSLI, just like historical CSLI, should be protected by the Fourth Amendment and that a warrant should be required before law enforcement may obtain it.

Part II of this Note describes how cell phones operate, what CSLI is, and how CSLI is collected. Part III analyzes the development of Fourth Amendment jurisprudence through *Carpenter*. Part IV explains the current state of the law and demonstrates, through three case illustrations, that lower courts are split on how to interpret the *Carpenter* decision. Part V sets out the proper way of interpreting *Carpenter* and how states can expedite the process of properly protecting their citizens. Lastly, Part VI concludes that the majority of lower courts are moving in the correct direction and that there is hope in the near future that all citizens will be properly protected against warrantless searches of their real-time CSLI.

II. CELL PHONES AND CELL-SITE LOCATION INFORMATION

A. The Ubiquitous Use of Cell Phones

There are 421.7 million wireless devices in the United States—nearly 1.3 devices for every person in the country.[11] In 2008, 77 percent of Americans owned a cell phone.[12] In 2019, it has risen to a staggering 96 percent, with 81 percent owning smartphones.[13] In addition, Americans are using their cell phones at unprecedented rates. Data usage is up over 73 times what it was in 2010 and continues to increase.[14] For example, from 2017 to 2018, there was an 82 percent

8. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001)).
9. 138 S. Ct. 2206 (2018).
10. *See id.* at 2223.
11. *2019 Annual Survey Highlights*, CTIA (June 20, 2019), https://www.ctia.org/news/2019-annual-survey-highlights.
12. *Mobile Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), https://www.pewinternet.org/fact-sheet/mobile.
13. *Id.*
14. *2019 Annual Survey Highlights*, *supra* note 11.

increase in mobile data use, which is "more data than was used in the first six and a half years of this decade—combined."[15]

Cell phones are a "pervasive and insistent part of daily life."[16] Not only does almost everyone own a cell phone, but people use them all day long, carry them everywhere they go, and rarely, if ever, turn them off. For example, 94 percent of smartphone owners "frequently" carry their phones,[17] 79 percent have their phones on or nearby for 22 hours a day,[18] and 82 percent never turn their phones off.[19]

B. How Cell Phones and CSLI Function

When cell phones are turned on, they continuously scan the environment in search of the best signal, which comes from the closest cell site.[20] Each time a cell phone "connects to a cell site, it generates a time-stamped record known as [CSLI]."[21] This information contains the time when the user connected to the site as well as the location of the site itself.[22] The record reveals "where the phone—and by proxy, its owner—is or has been," through "triangulating its precise location based on which cell sites receive" transmissions.[23]

Modern phones, such as smartphones, connect with cell sites "several times a minute,"[24] "but can connect as frequently as every seven seconds."[25] When smartphones connect to cell sites, they "generate location data even in the absence of any user interaction with the phone."[26] This occurs because smartphones have applications which continuously "run in the background," such as email applications.[27] Even turning off the location-privacy settings on the phone will not affect the service provider's ability to access CSLI.[28]

---

15. *Id.*
16. Riley v. California, 573 U.S. 373, 385 (2014).
17. LEE RAINIE & KATHRYN ZICKUHR, PEW RES. CTR., AMERICANS' VIEWS ON MOBILE ETIQUETTE 2 (2015), https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity.
18. Allison Stadd, *79% of People 18-44 Have Their Smartphones with Them 22 Hours a Day*, ADWEEK (Apr. 2, 2013, 12:00 PM), https://www.adweek.com/digital/smartphones.
19. RAINIE & ZICKUHR, *supra* note 17.
20. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
21. *Id.*
22. Brief of Amici Curiae Electronic Frontier Foundation et al., *supra* note 4, at 16.
23. *Id.* at 12, 16.
24. *Carpenter*, 138 S. Ct. at 2211.
25. Brief of Amici Curiae Electronic Frontier Foundation et al., *supra* note 4, at 16.
26. *Id.*
27. *Id.*
28. *Id.* at 9.

Thus, the only way phone users can protect their location data is to completely shut off their phones.[29]

The accuracy of the location information "depends on the size of the geographic area covered by the cell site."[30] The greater the concentration of cell sites, the more accurate the location data will be.[31] To handle the massive increase in cell phone usage, service providers are building more and more cell sites, which in turn creates more accurate CSLI.[32]

Generally, cell sites are mounted on towers.[33] However, more recently, they have been placed on "light posts, flagpoles, church steeples, [and] the sides of buildings."[34] As of 2018, there are 349,344 cell sites in the United States,[35] totaling more than a 52 percent growth over the last decade.[36] This substantial growth is not coming to an end. Analysts project that another 800,000 cell sites will be built in the next few years.[37] Even with the current 349,344 cell sites, CSLI is approaching GPS-level precision.[38] This means that CSLI can pinpoint a phone's location within a "few feet of its position," and will only become more accurate as more cell sites are created.[39]

Service providers collect and retain CSLI for several reasons and for various periods of time. For example, in its privacy statement, T-Mobile explains that:

> [i]f your mobile device is turned on, our network is collecting data about the device location. We may use, provide access to, or disclose this network location data without your approval to provide and support our services, including to route wireless communications, operate and improve our

29. RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE AT N.Y. UNIV. SCH. OF LAW, CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY: HOW THE GOVERNMENT IS COLLECTING AND USING YOUR LOCATION DATA 2 (2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Cell_Surveillance_Privacy.pdf ("[S]hort of turning off one's phone, it is nearly impossible to prevent the transmission of location data.").

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

31. *Id.* at 2211–12.

32. *Id.*

33. *Id.* at 2211.

34. *Id.*

35. *2019 Annual Survey Highlights*, *supra* note 11.

36. *2018 Annual Survey Highlights*, CTIA (July 10, 2018), https://www.ctia.org/news/the-state-of-wireless-2018.

37. *Id.*

38. *See* LEVINSON-WALDMAN, *supra* note 29, at 2.

39. *Id.* at 1.

> network and business, detect and prevent fraud, provide emergency responders information about how to find you when you call 911, or as required by law or emergency.[40]

Service providers will retain this data anywhere from three months to seven years.[41]

C. How Law Enforcement Uses CSLI

Law enforcement may obtain CSLI from service providers if it satisfies certain requirements. As mentioned above, prior to *Carpenter*, law enforcement could obtain CSLI with a court order under the Stored Communications Act.[42] The Stored Communications Act "permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'"[43] This "showing falls well short of the probable cause required for a warrant" and needed a change.[44] The Supreme Court, in *Carpenter*, attempted to make that change. However, it was not enough. The reason why the change was insufficient will be explained in Parts IV and V of this Note.

There are two types of CSLI which law enforcement may collect: "historical" CSLI and "real-time" CSLI.[45] Historical CSLI is location information collected by a service provider "in the past," or, in other words, "prior to the time of a data request."[46] This includes data that was collected "one day ago, one month ago, one year ago or beyond."[47] Law enforcement uses historical CSLI "to look back through service provider records to determine a suspect's location at a given point in the past."[48] This allows law enforcement to "prove that

40. *Privacy Policy*, T-MOBILE, https://www.t-mobile.com/responsibility/privacy/privacy-policy (last updated Dec. 21, 2019).

41. *Cellular Provider Record Retention Periods*, PROF. DIGITAL FORENSIC CONSULTING: BLOG (Apr. 5, 2017), https://prodigital4n6.com/cellular-provider-record-retention-periods (listing data retention periods for five different service providers).

42. *See* 18 U.S.C. § 2703(d) (2012).

43. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (quoting 18 U.S.C. § 2703(d)).

44. *Id.* at 2221.

45. State v. Andrews, 134 A.3d 324, 328 n.3 (Md. Ct. Spec. App. 2016).

46. *Cell Site Location Information: What Is It?*, ELECTRIC FRONTIER FOUND.: CRIM. DEFENDER TOOLKIT, https://www.eff.org/criminaldefender/cell-site-location (last visited Nov. 15, 2019).

47. *Id.*

48. *Andrews*, 134 A.3d at 328 n.3.

a defendant was in the area where a crime of which he is accused occurred."[49]

Real-time CSLI is "current or future location information . . . that live-tracks a cell phone's location at any given moment."[50] Law enforcement uses real-time CSLI "to track the whereabouts and movements of a suspect by using the cell phone as a tracking device."[51] It is commonly used to assist law enforcement in locating a suspect to make an arrest.[52]

There are two main methods by which law enforcement collect historical CSLI. First, and most commonly, law enforcement will request past location information from a service provider for *particular* cell phone numbers.[53] The other method, called "cell tower dumps," is where law enforcement agencies "request information about *every* device connected to a single tower during a particular interval, potentially netting historical location information from thousands of phones."[54]

There are also two main methods in which law enforcement collects real-time CSLI. The first method, called "pinging," is where law enforcement requests that service providers "'ping' phones to force them into revealing their location."[55] Pinging "relies on Enhanced 911 (E911) data, which allows law enforcement to pinpoint the location of cell phones that have placed 911 calls."[56] However, the "provider can also make a reverse 911 call, allowing the police to invisibly track a target's cell phone in real time."[57] The second method, the use of "cell-site simulators" or "Stingrays," effectively allows law enforcement to "circumvent the service provider and gain direct access to real-time" CSLI.[58] The device "'masquerades as a cell tower, tricking all nearby cell phones to connect to itself' rather than

49. *Id.*
50. *Cell Site Location Information: What Is It?*, *supra* note 46.
51. *Andrews*, 134 A.3d at 328 n.3.
52. Primer from Nat'l Ass'n of Criminal Def. Lawyers on Cell Phone Location Tracking (June 7, 2016), https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf.
53. LEVINSON-WALDMAN, *supra* note 29, at 2.
54. *Id.*
55. *Id.*; *Cellular Provider Record Retention Periods*, *supra* note 41.
56. LEVINSON-WALDMAN, *supra* note 29, at 2.
57. *Id.*
58. *Id.*

to a legitimate tower."[59] When used, "whether by hand, from within a patrol car, or attached to a plane," the device gathers the real-time CSLI "of all phones within range."[60]

Law enforcement agencies frequently collect CSLI. For example, in 2018, T-Mobile received 104,221 requests for CSLI.[61] In particular, it received 70,224 historical requests, 6,184 tower dump requests, and 27,813 real-time requests.[62] Additionally, in just the first half of 2019,[63] AT&T received 47,110 requests for CSLI.[64] In particular, it received 37,144 historical requests, 1,497 tower dump requests, and 8,469 real-time requests.[65]

III. EXISTING FOURTH AMENDMENT LAW IMPACTING CSLI

The distinction between historical CSLI and real-time CSLI has significant legal ramifications when it comes to Fourth Amendment protection. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[66] However, courts have struggled with determining whether CSLI is protected by the Fourth Amendment because CSLI does "not fit neatly under existing [Fourth Amendment] precedents."[67]

In legal terms, CSLI is defined as "personal location information maintained by a third party."[68] The "personal location information," refers to the time-stamped record generated each time the cell phone connects to a cell site, and the "third party" refers to a cell-phone provider, such as Verizon, T-Mobile, or Sprint.[69]

---

59. *Id.* (quoting George Joseph, *Cellphone Spy Tools Have Flooded Local Police Departments*, CITYLAB (Feb. 8, 2017), https://www.citylab.com/equity/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/).

60. *Id.*

61. T-MOBILE U.S., TRANSPARENCY REPORT FOR 2018 6 (2018), https://www.t-mobile.com/content/t-mobile/corporate/news/media-library/details/document.html/content/dam/t-mobile/corporate/media-library/public/documents/TransparencyReport2018.pdf?a=b.

62. *Id.*

63. From January to June 2019. *See* AT&T INTELLECTUAL PROP., AUGUST 2019 TRANSPARENCY REPORT 4 (2019), https://about.att.com/ecms/dam/csr/2019/library/ATT_English_TransparencyReport_Aug%202019.pdf.

64. *Id.*

65. *Id.*

66. U.S. CONST. amend. IV.

67. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

68. *Id.*

69. *See id.* at 2211–12.

This definition of CSLI creates an issue for the courts because CSLI falls between "two lines of cases."[70] One line of cases holds a person has "a reasonable expectation of privacy in the whole of their physical movements."[71] The second line of cases abides by the "third-party" doctrine, which states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[72]

Various courts around the country have struggled to determine what precedent controls the "unique nature" of CSLI.[73] However, in 2018, the Supreme Court had the opportunity to address this question. In *Carpenter v. United States*, the Court held "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [historical] CSLI," and that "accessing seven days of CSLI constitute[d] a Fourth Amendment search."[74] However, the Court did not express whether this protection applie[d] to real-time CSLI and "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny."[75]

This extremely narrow holding effectively "raise[d] more questions than it answer[ed]."[76] Most importantly, *Carpenter* left it to the lower courts to interpret whether the Fourth Amendment protects real-time CSLI and whether there is a limited time for which either type of CSLI may be obtained without a warrant.[77] Several lower courts have addressed these questions; however, there are major splits on when, if ever, individuals maintain a legitimate expectation of privacy in their real-time CSLI.[78]

---

70. *Id.* at 2214–15.

71. *Id.* at 2215, 2217.

72. *Id.* at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)); *see also* Sims v. State, 569 S.W.3d 634, 643 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019) ("To resolve the expectation-of-privacy issue in this case, we must consider two different lines of Supreme Court jurisprudence . . . .").

73. *See Carpenter*, 138 S. Ct. at 2217.

74. *Id.* at 2217, 2217 n.3.

75. *Id.* at 2217 n.3.

76. Vanessa Blum, *What's Next for Digital Privacy? New Clashes over the Fourth Amendment*, LAW.COM: RECORDER (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.

77. *See Carpenter*, 138 S. Ct. at 2217 n.3, 2220.

78. *See* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 947, 950 n.33 (2019) (organizing lower courts' interpretations of *Carpenter* into four differing models).

When the opportunity again arises for the Supreme Court to address whether real-time CSLI is protected by the Fourth Amendment, the Court should hold that individuals have a reasonable expectation of privacy in their real-time CSLI and that a warrant should be required to access it. A brief background of the Fourth Amendment and its evolution towards *Carpenter* is helpful in understanding why this should be so.

A. The Fourth Amendment and Katz v. United States

As mentioned above, the Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[79] Traditionally, the Fourth Amendment was "tied to common-law trespass," where unreasonable searches consisted of "*physically intruding* on a constitutionally protected area," such as the home.[80] However, in *Katz v. United States*,[81] the Supreme Court drastically expanded the conception of the Fourth Amendment to protect an individual's "reasonable expectation" of privacy rather than mere "places."[82]

In 1967, the Supreme Court, in *Katz*, "laid the groundwork for the 'reasonable expectation of privacy' test."[83] There, law enforcement, without a warrant, attached an eavesdropping device to the top of a public telephone booth to listen to and record the defendant's conversation.[84] The prosecution later used this conversation as evidence at trial.[85] The defendant argued that the device constituted a search and violated the Fourth Amendment because it invaded the privacy he "justifiably relied" on when using the phone booth.[86] The government argued the device did not violate the Fourth Amendment because it "involved no physical penetration of the telephone booth."[87]

The Court sided with the defendant and famously stated that the Fourth Amendment "protects people, not places."[88] This meant that the Fourth Amendment was not *only* violated when there was a

79. U.S. CONST. amend. IV.
80. *Carpenter*, 138 S. Ct. at 2213 (emphasis added).
81. 389 U.S. 347 (1967).
82. *Id.* at 351.
83. Tracey v. State, 152 So. 3d 504, 512 (Fla. 2014).
84. *Katz*, 389 U.S. at 348–49.
85. *Id.*
86. *Id.* at 353.
87. *Id.* at 352.
88. *Id.* at 351.

"physical intrusion" of a protected area.[89] Instead, the Fourth Amendment was also violated when the defendant's "reasonable expectation of privacy" was invaded.[90]

Justice Harlan, in a concurrence, fleshed out what the Supreme Court has subsequently adopted as the "reasonable expectation of privacy" test.[91] The test consists of a two-part inquiry: (1) has the individual manifested a subjective expectation of privacy, and (2) "is society willing to recognize that expectation as reasonable?"[92]

There is no definitive list as to what expectations of privacy are "reasonable." However, cases following *Katz*, such as *United States v. Knotts*[93] and *United States v. Jones*,[94] where law enforcement used tracking devices to follow the defendants' vehicles, demonstrate how the Supreme Court has applied the *Katz* "reasonable expectation of privacy" test to a person's expectation of privacy in his physical location and movements.[95]

B. An Individual's Expectation of Privacy in His or Her Physical Location and Movements

1. *United States v. Knotts*

In 1983, the Supreme Court, in *Knotts*, held that a law enforcement "beeper" did not violate the defendant's "reasonable expectation of privacy."[96] There, law enforcement believed the defendant was purchasing chloroform to produce illegal drugs.[97] Then, without a warrant, law enforcement placed a beeper—a tracking device—inside a chloroform container that was later sold to the

89. *Id.* at 352–53.

90. *Id.* at 360–61 (Harlan, J., concurring).

91. Tracey v. State, 152 So. 3d 504, 512 (Fla. 2014); *see also* United States v. Jones, 565 U.S. 400, 406 (2012) (stating that in "later cases" the Supreme Court has "applied the analysis of Justice Harlan's concurrence . . . which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy'").

92. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *see also* California v. Ciraolo, 476 U.S. 207, 211 (1986) (reiterating the test as "first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?").

93. 460 U.S. 276 (1983).

94. 565 U.S. 400 (2012).

95. *See id.* at 404; *Knotts*, 460 U.S. at 281.

96. *Knotts*, 460 U.S. at 281.

97. *Id.* at 278.

defendant.[98] Relying on the beeper's signal to keep the vehicle in view, law enforcement followed the defendant's vehicle carrying the chloroform from its place of purchase to the defendant's cabin.[99] Law enforcement then secured a search warrant for the cabin and discovered it was being used as a drug laboratory.[100]

The defendant argued the use of the beeper was prohibited by the Fourth Amendment because it violated his "reasonable expectation of privacy."[101] The Court applied the *Katz* "reasonable expectation of privacy" test and held the beeper did not violate the Fourth Amendment.[102] It stated that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" because the movements are "voluntarily conveyed to anyone who wants to look."[103]

However, the Court made clear that this was not a blanket rule for all future electronic-type tracking in public areas.[104] It explained that "different constitutional principles may be applicable" to "twenty-four hour surveillance of any citizen of this country."[105]

2. *United States v. Jones*

In 2012, the Supreme Court, in *Jones*, examined the "more sophisticated surveillance . . . envisioned in *Knotts* and found that different principles did indeed apply."[106] There, law enforcement believed the defendant was trafficking narcotics and, without a warrant, installed a tracking device on the defendant's vehicle.[107] Law enforcement tracked the defendant for twenty-eight days and found he was working at a narcotics stash house.[108] The defendant argued the placing of the tracking device on his vehicle violated the Fourth Amendment.[109]

98. *Id.* at 278–79.
99. *Id.*
100. *Id.* at 279.
101. *See id.*
102. *Id.* at 280–81, 285.
103. *Id.* at 281–82.
104. *See id.* at 283–84.
105. *Id.*
106. Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018); *see* United States v. Jones, 565 U.S. 400, 409–13 (2012).
107. *Jones*, 565 U.S. at 402–03.
108. *Id.* at 403–04.
109. *See id.* at 403.

The Supreme Court agreed.[110] However, instead of applying the *Katz* "reasonable expectation of privacy" test, the Court based its decision on the traditional "common-law trespass" approach.[111] It held the Fourth Amendment was violated because law enforcement physically intruded on the defendant's "personal property to gather information," and therefore it was not necessary to apply the *Katz* test.[112]

However, in the concurrences, five Justices agreed that, if the *Katz* "reasonable expectation of privacy" test was applied, "longer term GPS monitoring in investigations of most offenses impinges on the expectation of privacy—regardless whether those movements were disclosed to the public at large."[113] For example, the *Jones* Justices noted that the privacy concerns would be raised by conducting GPS tracking of the defendant's cell phone.[114]

Both *Knotts* and *Jones* recognized that individuals have a reasonable expectation of privacy in their physical movements.[115] However, as technology has advanced, this expectation of privacy has collided with the third-party doctrine.[116] To understand this conflict, it is helpful to understand the principles on which the third-party doctrine was formed.

C. The Third-Party Doctrine

The third-party doctrine is the notion that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[117] However, this doctrine is not as stringent as it sounds. The Supreme Court applied the third-party doctrine in *United States v. Miller*[118] and *Smith v. Maryland*,[119] and in doing so, the Court

110. *Id.* at 404.
111. *Id.* at 404–05.
112. *Id.* at 414 (Sotomayor, J., concurring).
113. Carpenter v. United States, 138 S. Ct. 2206, 2215 (2012) (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).
114. *Jones*, 565 U.S. at 426, 428 (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring).
115. *Carpenter*, 138 S. Ct. at 2215, 2217 (analyzing *Knotts* and *Jones* decisions).
116. *See id.* at 2214 (explaining that "personal location information maintained by a third party does not fit neatly under existing precedents" but "lie[s] at the intersection of two lines of cases").
117. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
118. 425 U.S. 435 (1976).
119. 442 U.S. 735 (1979).

did not "rely solely on the act of sharing," but rather, it considered "the *nature* of the particular documents sought."[120]

1. *United States v. Miller*

In 1976, the Supreme Court, in *Miller*, held the defendant had no expectation of privacy in financial records voluntarily conveyed to a bank.[121] There, the defendant was under investigation for tax fraud, and law enforcement used an allegedly defective subpoena to obtain his bank records.[122] The defendant argued that obtaining his records with a defective subpoena violated his Fourth Amendment rights.[123] However, the Court disagreed and held the defendant had "no legitimate 'expectation of privacy' in" the records.[124]

The Court applied the *Katz* "reasonable expectation of privacy" test and laid out two reasons why the defendant had no expectation of privacy.[125] First, the Court looked to the "nature of the [records]."[126] It determined the records were not "private papers," but rather non-confidential "negotiable instruments to be used in commercial transactions."[127] Second, the Court explained the records were "voluntarily conveyed to the banks . . . in the ordinary course of business," and that the "Fourth Amendment does not prohibit the obtaining of information revealed to a third party"[128] because "(w)hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[129] The Court concluded the defendant, by "revealing his affairs to another," had taken a risk that the information would be conveyed "to the Government."[130]

2. *Smith v. Maryland*

In 1979, the Supreme Court, in *Smith*, held the defendant had no expectation of privacy in his records of dialed telephone numbers

120. *Miller*, 425 U.S. at 442 (emphasis added); *see also* Smith, 442 U.S. at 742 (considering the nature of the information collected by the pen register).
121. *Miller*, 425 U.S. at 442–43.
122. *Id.* at 436.
123. *Id.* at 437.
124. *Id.* at 442.
125. *Id.* at 442–43.
126. *Id.* at 442.
127. *Id.* at 440–42.
128. *Id.* at 442–43.
129. *Id.* at 442 (alteration in original) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
130. *Id.* at 443.

voluntarily conveyed to a telephone company.[131] There, the defendant was a suspect in a robbery.[132] Law enforcement, without a warrant, had a pen register[133] installed on the defendant's home phone in order to record the numbers he dialed.[134] These records led to the defendant's eventual arrest and conviction.[135] The defendant argued the warrantless pen register violated his "legitimate expectation of privacy" in the "numbers he dialed on his phone."[136] However, the Court applied the *Katz* "reasonable expectation of privacy" test and rejected the defendant's argument.[137]

Similar to the Supreme Court's decision in *Miller*, the "nature" of the records was essential in the Court's decision.[138] The Court doubted that telephone users have "any [subjective] expectation of privacy regarding the numbers they dial" because of the very "limited capabilities" of pen registers.[139] The Court emphasized that pen registers "disclose *only* the telephone numbers that have been dialed."[140] In addition, the Court concluded, the "expectation [was] not 'one that society is prepared to recognize as reasonable,'"[141] because the defendant "voluntarily conveyed" the dialed numbers and "assumed the risk that the information would be divulged to police."[142]

The third-party doctrine receives more and more criticism as technology advances. In the 1970s, when *Miller* and *Smith* were decided, it made sense that records with very "limited capabilities," such as records of dialed numbers and bank records, did not have protection when voluntarily conveyed to a third-party.[143] But now, the "nature" of the information being conveyed is much more detailed and intimate. Law enforcement no longer seizes records of dialed

131. Smith v. Maryland, 442 U.S. 735, 744 (1979).
132. *Id.* at 737.
133. To be clear, "pen registers do not acquire the *contents* of communications . . . '[t]hey disclose only the telephone numbers that have been dialed.'" *Id.* at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).
134. *Id.* at 737.
135. *Id.* at 737–38.
136. *Id.* at 742.
137. *See id.* at 740, 745.
138. *See id.* at 741–42.
139. *Id.* at 742.
140. *Id.* at 741 (emphasis added).
141. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).
142. *Id.* at 745.
143. *See id.* at 744–45.

numbers, but instead, seizes an individual's exact location, within a few feet.

The expectation of privacy in an individual's physical location and movements, delineated in *Knotts* and *Jones*, has collided with the third-party doctrine of *Miller* and *Smith*. Which doctrine gives way? The Supreme Court confronted this conflict in *Carpenter* and attempted to demonstrate how these principles interact. However, the Court's resolution ended up "rais[ing] more questions than it answer[ed]."[144]

D. Carpenter v. United States

On June 22, 2018, the Supreme Court, in the landmark case of *Carpenter v. United States*, held that "accessing seven days of [historical] CSLI constitute[d] a Fourth Amendment search."[145] There, law enforcement arrested four men suspected of committing a string of armed robberies.[146] One of these men confessed and gave law enforcement the phone numbers of other alleged accomplices, including the cell phone number of the defendant, Timothy Carpenter.[147] Shortly after, law enforcement obtained a court order under the Stored Communications Act to obtain seven days of Carpenter's historical CSLI from the service provider Sprint.[148]

The prosecution used the seven days of historical CSLI at trial to show that Carpenter's phone was "near four of the charged robberies" at the time those robberies occurred.[149] This evidence led to the eventual conviction of Carpenter and a prison sentence of over one hundred years.[150]

Carpenter appealed the conviction to the Sixth Circuit and argued that law enforcement's seizure of the historical CSLI "violated the Fourth Amendment because [it] had been obtained without a warrant

144. Blum, *supra* note 76.

145. Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

146. *Id.* at 2212.

147. *Id.*

148. *Id.* The Stored Communications Act allows the government to obtain CSLI by simply showing that the records are "relevant and material to an ongoing investigation," which is a much lower showing than the probable cause required for a warrant. *Id.* at 2221 (quoting 18 U.S.C. § 2703(d) (2012)).

149. *Id.* at 2213.

150. *Id.*

supported by probable cause."[151] The Sixth Circuit, citing *Smith*,[152] and applying the third-party doctrine, held that Carpenter "lacked a reasonable expectation of privacy in the location information . . . because he had *shared* that information with his wireless carriers."[153] The Supreme Court granted certiorari and was faced with determining whether "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[154]

As explained in Part III of this Note, the *Carpenter* Court had difficulties resolving this issue because CSLI "does not fit neatly under existing precedent" but instead "lie[s] at the intersection of two lines of cases."[155] The first set being *Knotts* and *Jones*, which addressed a "person's expectation of privacy in his physical location and movements," and the second set being *Miller* and *Smith*, which addressed the third-party doctrine.[156] The *Carpenter* Court explained that collection of CSLI has "many of the qualities of the GPS monitoring . . . considered in *Jones*."[157] However, it also "implicates the third-party principle of *Smith* and *Miller*" because "the individual continuously reveals his location to his wireless carrier."[158]

The collision of these two doctrines required the Court to address a novel issue. Which doctrine gives way? Does the fact CSLI is "shared" and "held" by a third party trump an individual's expectation of privacy in his or her physical location and movements? The Court did not think so. It "decline[d] to extend" the third-party doctrine to the collection of historical CSLI and held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements."[159] The Court organized its analysis into two parts. First, the Court applied the *Katz* "reasonable expectation of privacy" test. Second, the Court addressed whether the third-party doctrine extends to CSLI.

151. *Id.* at 2212.
152. *See supra* Part III (discussing the third-party doctrine).
153. *Carpenter*, 138 S. Ct. at 2213 (emphasis added) (discussing the Sixth Circuit's holding).
154. *Id.* at 2217.
155. *Id.* at 2214.
156. *Id.* at 2215–16.
157. *Id.* at 2216.
158. *Id.*
159. *Id.* at 2217.

1. Application of the "Reasonable Expectation of Privacy" Test

In applying the *Katz* "reasonable expectation of privacy" test, the Court looked to *Jones*. It found that *Jones*, rather than *Knotts*, controlled because *Knotts* dealt with a less sophisticated form of surveillance distinguishable from CSLI.[160] It began by acknowledging that a majority of the Supreme Court, in both *Jones* and *Knotts*, have "already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[161] However, the *Carpenter* Court took this expectation much further.

The Court explained that CSLI "hold[s] for many Americans the 'privacies of life.'"[162] It stated that CSLI is an "all-encompassing record" which "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[163] It reasoned that collection of CSLI "present[s] even greater privacy concerns than the GPS monitoring . . . in *Jones*."[164] This was because cell phones are a "feature of human anatomy," and unlike the GPS monitoring of a vehicle in *Jones*, individuals "regularly" and "compulsively" bring their cell phones with them everywhere.[165] This allows law enforcement to monitor far beyond "public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[166]

The Court concluded that, with CSLI, law enforcement had "access to a category of information otherwise unknowable"; it "can now travel back in time to retrace a person's whereabouts," and the only restraint is the length of time the data is retained by wireless carriers.[167] Accordingly, the Court held that it was reasonable for society to expect that law enforcement will not "catalogue every single

160. *See id.* at 2218. (explaining that "[u]nlike the bugged container in *Knotts* . . . a cell phone . . . tracks nearly exactly the movements of its owner").

161. *Id.* at 2217.

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

163. *Id.* (quoting United States v. Jones, 565 U.S. 400, 402–03 (2012) (Sotomayor, J., concurring)).

164. *Id.* at 2218.

165. *Id.* (quoting *Riley*, 573 U.S. at 385).

166. *Id.*

167. *Id.* ("[W]ireless carriers . . . currently maintain records for up to five years.").

movement" of an individual,[168] and that allowing law enforcement to access CSLI "contravenes that expectation."[169]

2. Application of the Third-Party Doctrine

Next, the Court moved to the second part of its analysis: application of the third-party doctrine. In doing so, the Court addressed the two rationales behind the third-party doctrine: "the nature of the particular documents"[170] and "voluntary exposure."[171]

The Court began by addressing the "nature of the particular documents."[172] The government argued that the third-party doctrine should be applied to CSLI because, like the dialed numbers and bank records in *Smith* and *Miller*, CSLI are "'business records' created and maintained by the wireless carriers."[173] However, the Court disagreed because the government failed to acknowledge the "*seismic shifts*"[174] in surveillance technology that allowed law enforcement to track "not only Carpenter's location but also everyone else's, not for a short period but for years and years."[175]

Furthermore, the Court distinguished CSLI from the "limited types of personal information" sought in *Smith* and *Miller*.[176] It found there was a "world of difference" between dialed numbers and bank records, and the "exhaustive chronicle of location information casually collected by wireless carriers."[177] While dialed numbers and bank records "reveal little in the way of 'identifying information,'"[178] CSLI has "no comparable limitations on [its] revealing nature."[179] CSLI discloses a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[180] Thus, the Court concluded that due to the "nature" of CSLI, the government

168. *Id.* at 2217; *see* Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, LAWFARE: BLOG (June 22, 2018, 2:05 PM), https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

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

170. *Id.* at 2219 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

171. *Id.* at 2220.

172. *Id.* at 2219.

173. *Id.*

174. *Id.* (emphasis added).

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)).

179. *Id.*

180. *Id.* at 2220.

"[was] not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information."[181]

Next, the Court moved to the second rationale underlying the third-party doctrine: "voluntary exposure."[182] The Court explained that CSLI "is not truly 'shared' as one normally understands the term."[183] CSLI is generated by "[v]irtually any activity on the phone," including "incoming calls, texts, or e-mails," and therefore can be generated "without any affirmative act on the part of the user beyond powering up."[184] Furthermore, cell phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[185] Thus, the Court concluded that "there is no way to avoid leaving behind a trail of location data,"[186] and "in no *meaningful* sense does the user voluntarily 'assume[] the risk'" of sharing the data.[187] Consequently, the Court declined to extend the third-party doctrine to the collection of historical CSLI.[188]

3. The Supreme Court's Holding

Accordingly, the Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[189] However, in controversial fashion, the Court made clear its decision was "a narrow one."[190] The Court stated that its holding did not apply to "*real-time* CSLI" and did not decide whether there was a limited period for which law enforcement may obtain an individual's historical CSLI without a warrant.[191] It stated that it was "sufficient for our purposes . . . to hold that accessing *seven days* of CSLI constitute[d] a Fourth Amendment search."[192]

181. *Id.* at 2219.
182. *Id.* at 2220.
183. *Id.*
184. *Id.*
185. *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
186. *Id.*
187. *Id.* (emphasis added) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).
188. *See id.*
189. *Id.* at 2217.
190. *Id.* at 2220.
191. *See id.* (emphasis added).
192. *Id.* at 2217 n.3 (emphasis added).

Therefore, the Supreme Court left it to the lower courts to interpret whether individuals maintain a legitimate expectation of privacy in their *real-time* CSLI and whether accessing less than *seven days* of CSLI constitutes a search.[193]

IV. INTERPRETATIONS OF *CARPENTER V. UNITED STATES*

Several lower courts have addressed whether the protections of *Carpenter* extend to real-time CSLI and whether accessing less than *seven days* of CSLI constitutes a search. However, the lower courts are split on when, if ever, individuals maintain a legitimate expectation of privacy in their real-time CSLI.[194] There are three lower court decisions that demonstrate the wide-ranging interpretations of *Carpenter*: *Andres v. State*,[195] *Sims v. State*,[196] and *Commonwealth v. Almonor*.[197]

In *Andres*, the Supreme Court of Florida held the *Carpenter* ruling did not apply to real-time CSLI.[198] In *Sims*, the Texas Criminal Appeals Court held an individual did not have a reasonable expectation of privacy in three hours of real-time CSLI.[199] And, in *Almonor*, the Supreme Court of Massachusetts held that collection of *any* CSLI intruded on a person's reasonable expectation of privacy.[200]

A. Andres v. State

In September 2018, the Supreme Court of Florida decided *Andres* and found the *Carpenter* holding inapplicable because Florida law enforcement had used real-time CSLI to locate the defendant.[201]

193. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1191 n.8 (Mass. 2019) (explaining that the Supreme Court "expressly avoided" addressing the protection of real-time CSLI).

194. *See* Rozenshtein, *supra* note 78, at 950–51.

195. 254 So. 3d 283 (Fla. 2018).

196. 569 S.W.3d 634 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019).

197. 120 N.E.3d 1183 (Mass. 2019).

198. *Andres*, 254 So. 3d at 297 n.7.

199. *Sims*, 569 S.W.3d at 646.

200. *See Almonor*, 120 N.E.3d at 1195–96; *see also* Jennifer Lynch, *Massachusetts Court Blocks Warrantless Access to Real-Time Cell Phone Location Data*, ELECTRONIC FRONTIER FOUND. (Apr. 24, 2019), https://www.eff.org/deeplinks/2019/04/massachusetts-court-blocks-warrantless-access-real-time-cell-phone-location-data (explaining that the Supreme Court of Massachusetts held that "police access to real-time cell phone location data—whether it comes from a phone company or from technology like a cell site simulator—intrudes on a person's reasonable expectation of privacy").

201. *Andres*, 254 So. 3d at 297 n.7; *see also* Peter A. Crusco, *'*Carpenter*' Squared: Review and Reconcile State Court Cases Impacted by Landmark SCOTUS Decision*, LAW.COM: N.Y.L.J. (Apr. 22, 2019, 2:50 PM), https://www.law.com/newyorklawjournal/2019/04/22/carpenter-

There, the defendant was a suspect in a murder case, and law enforcement obtained a warrant to search the defendant's body, home, and van.[202] Law enforcement then used a cell-site simulator, or Stingray, to locate the defendant and execute the warrant.[203] Upon finding and arresting the defendant, law enforcement took a DNA sample as well as photographs of his body, which led to the defendant's eventual conviction.[204]

The defendant attempted to suppress this evidence by arguing that an additional "probable cause warrant was required" to use the cell-site simulator.[205] The court rejected the argument. It held that the evidence obtained—the DNA and photographs—was "well within the scope of the [original] warrant" and an additional warrant was not needed.[206] In coming to this decision, the court explicitly stated that the *Carpenter* "holding [was] not applicable . . . [because] officers used real-time cell-site location information."[207]

B. Sims v. State

In January 2019, the Texas Criminal Appeals Court decided *Sims* and held that three hours of real-time CSLI tracking did not intrude on the legitimate expectation of privacy afforded by the Fourth Amendment.[208] The defendant, a murder suspect, was identified driving the victim's vehicle and using the victim's credit cards.[209] The officer who made this discovery went back to his office to obtain a warrant to ping the defendant's cell phone.[210] However, upon arrival, he discovered that another officer had already done so without a proper warrant.[211] The warrantless pinging allowed law enforcement to track

squared-review-and-reconcile-state-court-cases-impacted-by-landmark-scotus-decision ("The court concluded that *Carpenter* was inapplicable because the officers used the simulator to obtain real-time cell site location information to locate Andres and execute the warrant.").

202. *Andres*, 254 So. 3d at 291, 297.

203. *Id.* at 297.

204. *Id.*

205. *Id.*

206. *Id.* at 298.

207. *Id.* at 297 n.7.

208. Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019); *see also* Benson Varghese, Sims v. State*: Can Police Obtain Real-Time Cell Site Location Without Warrant?*, VARGHESE SUMMERSETT: BLOG (Mar. 2, 2019), https://www.versustexas.com/criminal/sims-v-state (explaining the *Sims* decision).

209. *Sims*, 569 S.W.3d at 638.

210. *Id.*

211. *Id.*

the defendant in real-time, and led to the defendant's arrest and the discovery of key evidence.[212] The defendant moved to suppress the evidence and argued that accessing his real-time CSLI without a warrant violated his Fourth Amendment rights.[213]

The court looked to *Carpenter* to determine whether obtaining real-time CSLI records without a warrant violated the Fourth Amendment.[214] It began by stating that there was no difference between real-time and historical CSLI records when it came to Fourth Amendment protection and applying *Carpenter*.[215] In fact, the court hinted that real-time CSLI may be *even more* intrusive due to the fact that real-time records "are generated solely at the behest of law enforcement."[216]

However, the court then applied a unique test, which was inconsistent with *Carpenter*. It explained that when defining Fourth Amendment protection, it is not the "content," or the "nature," of the CSLI records that matters.[217] Instead, it is whether the government seized "enough" information to violate a legitimate expectation of privacy.[218] The court looked to "how long" law enforcement tracked a person.[219] It explained there is "no bright-line rule for determining how long police must track a person's cell phone in real time before it violates a person's legitimate expectation of privacy in those records," but rather, it "must be decided on a case-by-case basis."[220]

The *Sims* court explained that the *Carpenter* Court was "not totally clear" when it held that Fourth Amendment rights were violated when "*at least* seven days" of CSLI was accessed.[221] It argued that the Court "might have meant that accessing less than seven days of historical CSLI *could* also violate" the Fourth Amendment, or "it

212. *Id.* at 639.
213. *Id.* at 637.
214. *See id.* at 645.
215. *Id.*
216. *Id.* at 645 n.15.
217. *Id.* at 645–46; *see also* Varghese, *supra* note 208 ("In determining whether obtaining real-time CSLI records violated the Fourth Amendment, the Court looked to *Carpenter* and determined that what mattered was not the content of the CSLI records, but rather was whether the government seized 'enough' information from the records that it violated a legitimate expectation to privacy.").
218. *Sims*, 569 S.W.3d at 645–46.
219. *Id.* at 646.
220. *Id.*
221. *Id.* at 646 n.17.

might have meant that a person has [an] expectation of privacy in seven days or more of CSLI, but no less."[222]

Then, very abruptly, and with very little explanation, the *Sims* court concluded that the defendant "did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours of real-time CSLI records accessed by police by pinging his phone less than five times."[223] The court referred to *Carpenter* to explain that "longer-term surveillance might infringe on a person's legitimate expectation of privacy if the location records reveal the 'privacies of [his] life,' but this [was] not that case."[224]

C. Commonwealth v. Almonor

In April 2019, the Supreme Court of Massachusetts decided *Almonor*, and extended warrant protections to all real-time CSLI, no matter the type or how long the individual was tracked.[225] There, the defendant was a murder suspect and law enforcement warrantlessly pinged his cell phone in an effort to locate him.[226] The pinging allowed law enforcement to find the defendant and the murder weapon.[227]

The defendant moved to suppress the evidence, arguing that law enforcement pinging his "cell phone to reveal its real-time location constitute[d] a search" under the Fourth Amendment and Article 14 of the Massachusetts Declaration of Rights ("Article 14").[228] The court agreed and held the pinging constituted a search under Article 14.[229]

Although the defendant brought both federal and state constitutional claims, the court based its decision solely on Article 14.[230] However, for the purposes of this Note, the arguments and

222. *Id.*

223. *Id.* at 646.

224. *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)). Going even further, the court noted that prior to *Carpenter* it held, in *Ford v. State*, 477 S.W.3d 321 (Tex. Crim. App. 2015), that a "warrantless search of four days of historical CSLI did not violate the Fourth Amendment." *Id.* at 645 n.16. The court stated this holding was "prescient" and still valid because *Carpenter* only held "police needed a warrant to access seven days of historical CSLI, which was three days more than in *Ford*." *Id.*

225. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1195–96 (Mass. 2019).

226. *Id.* at 1187.

227. *Id.*

228. *Id.* at 1188.

229. *Id.*

230. *See id.* at 1191 n.9 ("[A]s we conclude that a ping is a search under art. 14, 'we have no need to wade into these Fourth Amendment waters.' Instead we 'decide the issue based on our State

points made by the court in support of the protection of real-time CSLI under Article 14 should, and could, be directly applied to Fourth Amendment protection.[231] In fact, the lower court judge concluded that the ping was a search under the Fourth Amendment,[232] and most of the Massachusetts Supreme Court's analysis entails looking to cases interpreting the Fourth Amendment.[233]

The State raised two arguments in defense of its warrantless ping of the defendant's phone. First, it argued that the defendant had no reasonable expectation of privacy in his cell phone's real-time CSLI.[234] Second, citing *Commonwealth v. Estabrook*[235]—a pre-*Carpenter* case—it argued CSLI could be obtained without a warrant as long as it was less than six hours.[236] However, the court rejected both arguments.[237]

In applying the *Katz* "reasonable expectation of privacy" test, the court focused on "the nature of intrusion."[238] In particular, the court emphasized that pinging was "initiated and effectively controlled by the police, and [was] done without any express or implied authorization or other involvement by the individual cell phone user."[239] The court explained that law enforcement's ability to obtain real-time CSLI was an "extraordinarily powerful surveillance tool [that] finds no analog in the traditional surveillance methods," such as patrolling streets, interviewing individuals, and knocking on doors to locate persons of interest.[240] For this reason, the court held that

---

Constitution . . . .'" (citations omitted) (first quoting Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014), and then quoting Commonwealth v. Mauricio, 80 N.E.3d 318 (Mass. 2017)).

231. *See* Lynch, *supra* note 200 (Article 14 of the Massachusetts Declaration of Rights "was drafted before—and served as one of the models for—our federal Bill of Rights. Article 14, one of the cornerstones of the Massachusetts Constitution, is the state's equivalent to the Fourth Amendment.").

232. *Almonor*, 120 N.E.3d at 1190 (explaining that after a three-day evidentiary hearing, "the motion judge concluded that the ping of the defendant's cell phone was a search under the Fourth Amendment").

233. *Id.* at 1191 n.9 (explaining that the court looked to cases interpreting the Fourth Amendment, such as *Katz*, *Jones*, and *Carpenter*, for "historical context and more general guidance").

234. *See id.* at 1196–97.

235. 38 N.E.3d 231 (Mass. 2015).

236. *Almonor*, 120 N.E.3d at 1196–97 (citing *Estabrook*, 38 N.E.3d at 237 (holding that law enforcement "may obtain historical CSLI for a period of six hours or less relating to an identified person's cellular telephone from the cellular service provider without obtaining a search warrant")).

237. *See id.* at 1193, 1997.

238. *Id.* at 1192.

239. *Id.* at 1193.

240. *Id.* at 1194–95.

"society's expectation has been that law enforcement could not secretly and instantly identify a person's real-time physical location at will," and 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 contravene[d] that expectation."[241]

In addition, the court noted that "[m]anipulating our phones for the purpose of identifying and tracking our personal location present[ed] an even greater intrusion"[242] than "accessing the historical location data at issue in *Carpenter*."[243] This is because "cell phones are 'an indispensable part of' daily life,"[244] and therefore the "ability to identify a cell phone's real-time location is . . . the ability to identify the real-time location of its user."[245]

Additionally, the court held the "six-hour rule" from *Estabrook* only applied to historical "telephone call" CSLI, rather than real-time CSLI.[246] The court explained that there were "fundamental differences" between historical "telephone call" CSLI, which is collected and stored by service providers when a cell phone user voluntarily makes or receives a telephone call, and "police action that causes a cell phone to identify its real-time location."[247] However, this analysis is flawed because historical CSLI is not only created when a user makes or receives a phone call. Instead, historical CSLI may be created even if the owner is not using the phone at all.[248]

The court should have held that the six-hour rule does not apply to any collection of CSLI. However, besides the six-hour rule holding, the Massachusetts Supreme Court got it right. Unlike the Supreme Court in *Carpenter*, the Massachusetts Supreme Court left no questions unanswered. It "confidently" held that collection of *any* CSLI—whether it comes from a service provider's historical phone

241. *Id.* at 1195.
242. *Id.* at 1194.
243. Lynch, *supra* note 200.
244. *Almonor*, 120 N.E.3d at 1194 (quoting Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014)).
245. *Id.*
246. *Id.* at 1197.
247. *Id.*
248. *See* Brief of Amici Curiae Electronic Frontier Foundation et al., *supra* note 4, at 16 (explaining that smartphones "generate location data even in the absence of any user interaction with the phone").

records or from technology like a cell-site simulator—intruded on a person's reasonable expectation of privacy.[249]

V. WHY REAL-TIME CSLI SHOULD BE PROTECTED AND WHAT TO EXPECT GOING FORWARD

Andres and *Sims* are great examples of how an individual's rights may be violated after the Supreme Court avoids addressing an important question. Hopefully, in the near future, the right case will reach the Supreme Court so that it can resolve this issue. However, in the meantime, lower courts should follow the lead of the Massachusetts Supreme Court in *Almonor* and hold that individuals have a reasonable expectation of privacy in their real-time CSLI.[250] Further, the courts should hold that a warrant is required to access CSLI for any period of time. In addition, state legislators should take matters into their own hands and pass legislation prohibiting the collection of *all* CSLI without a warrant.

Carpenter and *Almonor* got several things right. However, each had its flaws. Going forward, courts must recognize these flaws when addressing the protections of CSLI. Courts must acknowledge two main points: (1) although the *Carpenter* decision involved historical CSLI, the rule articulated by the United States Supreme Court—that collection of historical CSLI from third-party phone companies is a Fourth Amendment search that requires a warrant—should apply equally to the collection of real-time CSLI; and (2) although the *Carpenter* decision loosely held that a warrant is required only for collection of more than seven days of CSLI, a person's privacy interest in CSLI should not be limited by time.

A. The Protections of Carpenter *Should Apply to Real-Time CSLI*

When it comes to determining (1) whether a person has a legitimate expectation of privacy in real-time CSLI, and (2) whether the third-party doctrine should apply, there is "no difference" between historical and real-time CSLI.[251]

249. *Almonor*, 120 N.E.3d at 1197.

250. *See id.*

251. *See* Sims v. State, 569 S.W.3d 634, 645 n.15 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019) (explaining that for purposes of applying the third-party doctrine and for determining whether a person has a legitimate expectation of privacy in his physical movements and location, there is "no difference" between real-time and historical CSLI).

1. An Individual Has a Reasonable Expectation of Privacy in His or Her Real-Time CSLI

The application of the *Katz* "reasonable expectation of privacy" test to real-time and historical CSLI is very similar. Recall that the test has two prongs: first, the individual must have a subjective expectation of privacy; and second, the expectation must be reasonable.[252] In most cases, the subjective expectation is easily met because courts recognize that "no one buys a cell phone to share detailed information" with law enforcement.[253] Thus, the bulk of the analysis is dedicated to determining whether the expectation was reasonable.

The Supreme Court in *Carpenter* confirmed that it is society's expectation that law enforcement will not "catalogue every single movement" of an individual.[254] The Court held that allowing law enforcement to access historical CSLI without a warrant "contravene[d] that expectation."[255] How is the warrantless collection of real-time CSLI any different? The answer is, it is not. "Allowing law enforcement to immediately locate an individual whose whereabouts were previously unknown," and track his or her every movement "by compelling that individual's cell phone to reveal its location" *also* "contravenes that expectation."[256]

In *Carpenter*, the Court emphasized that the warrantless collection of historical CSLI "contravenes that expectation"[257] because historical CSLI can reach beyond areas of traditional surveillance.[258] In particular, it stated that a "cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[259] This reasoning also applies to the

252. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (requiring "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

253. State v. Earls, 70 A.3d 630, 643 (N.J. 2013).

254. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 430 (2012)); *see also* McCubbin, *supra* note 168 (explaining the *Carpenter* decision).

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

256. Commonwealth v. Almonor, 120 N.E.3d 1183, 1195 (Mass. 2019).

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

258. *See id.* at 2218 ("Unlike the bugged container in *Knotts*, or the car in *Jones*, a cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner." (citation omitted) (quoting Riley v. California, 573 U.S. 373, 385 (2014))).

259. *Id.*

collection of real-time CSLI, "because it, too, allows the government to follow people into homes and other private spaces."[260]

2. The Third-Party Doctrine Should Not Extend to the Collection of Real-Time CSLI

The Supreme Court—in *Miller*, *Smith*, and *Carpenter*—has made clear that the application of the third-party doctrine turns on two rationales: "the nature of the particular documents" and "voluntary exposure."[261]

a. Nature of real-time CSLI collection is more intrusive than historical CSLI collection

The nature of real-time CSLI collection is "not meaningfully different" than historical CSLI collection when it comes to applying the third-party doctrine.[262] In fact, in most cases, the nature of real-time CSLI collection is even more intrusive. Both historical and real-time CSLI are records of location information which hold the "privacies of life."[263] They are both "all-encompassing" records which may reveal a person's "familial, political, professional, religious, and sexual associations."[264] However, there is one significant difference that makes real-time CSLI even more invasive. Unlike historical CSLI, which are "business records" that are "maintained by cell phone service providers for business purposes, [and] are occasionally accessed by law enforcement, real-time CSLI records are generated solely at the behest of law enforcement."[265] In other words, service

260. Brief of Amici Curiae Electronic Frontier Foundation & American Civil Liberties Union of Massachusetts, Inc. et al., Commonwealth v. Almonor, 120 N.E.3d 1183 (Mass. 2019) (No. SJC-12499), 2018 WL 4154833, at *18.

261. *See Carpenter*, 138 S. Ct. at 2219–20 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)) (explaining that when applying the third-party doctrine courts do "not rely solely on the act of sharing," but rather, "they [also] consider[] 'the nature of the particular documents sought'" and limitations on any "legitimate 'expectation of privacy' concerning their contents"); Smith v. Maryland, 442 U.S. 735, 741, 743–44 (1979) (explaining that in applying the third-party doctrine "it is important to begin by specifying precisely the nature of the state activity that is challenged," as well as stating "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *Miller*, 425 U.S. at 442 (examining the "nature of the particular documents sought" and whether the information was "voluntarily conveyed" when applying the third-party doctrine).

262. Sims v. State, 569 S.W.3d 634, 645 n.15 (Tex. Crim. App. 2019), *cert. denied*, 139 S. Ct. 2749 (2019).

263. *Carpenter*, 138 S. Ct. at 2217 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

264. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

265. *Sims*, 569 S.W.3d at 645 n.15; *see Carpenter*, 138 S. Ct. at 2219.

providers do not collect or retain real-time CSLI. The *only* time it is collected is when law enforcement requests it.[266]

b. An individual does not voluntarily share real-time CSLI

The Supreme Court has held that historical CSLI is not "truly 'shared'" with the third-party cell service providers.[267] This decision was made even though historical CSLI may sometimes be generated by the affirmative action of the cell phone user, such as when the user makes a phone call or sends a text message.[268] However, unlike historical CSLI, real-time CSLI is *never* generated by the affirmative action of the cell phone user.[269]

As explained in Part II, there are two methods law enforcement use to collect real-time CSLI: pinging and cell-site simulators.[270] In both of these methods, law enforcement affirmatively compels a cell phone to transmit its real-time CSLI when it would not do so on its own.[271] In addition, when cell-site simulators are used, law enforcement does not need the assistance of a service provider whatsoever.[272] The simulators allow law enforcement to "circumvent the service provider and gain direct access to real-time" CSLI, therefore taking the third-party completely out of the equation.[273]

Accordingly, if the third-party doctrine does not extend to the collection of historical CSLI, it should not extend to the collection of real-time CSLI. While historical CSLI is sometimes shared with third-party service providers through the affirmative actions of users, real-time CSLI is never shared with a third-party service provider, and sometimes a third-party service provider is not even involved.

266. *See, e.g.*, Commonwealth v. Almonor, 120 N.E.3d 1183, 1193 (Mass. 2019) (explaining that "[w]ithout police direction, [real-time CSLI] would also not otherwise be collected and retained by the service provider").

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

268. *See id.* at 2212 ("While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections.").

269. *See Sims*, 569 S.W.3d at 645 n.15.

270. LEVINSON-WALDMAN, *supra* note 29, at 2; *see supra* Part II.

271. *See Sims*, 569 S.W.3d at 636 n.1 (explaining that when collecting real-time CSLI, law enforcement officers "proactively" identify a phone's real-time location "when the cell phone would not ordinarily transmit its location on its own").

272. *See* LEVINSON-WALDMAN, *supra* note 29, at 2.

273. *Id.*

B. An Individual's Privacy Interest in CSLI Should Not Be Limited by Time

The Texas Criminal Appeals Court in *Sims* was wrong when it held that the *Katz* "reasonable expectation of privacy" test turns on "how long" law enforcement tracks a person.[274] The collection of real-time CSLI "for even one data point is a search" and should require a warrant.[275] Like the courts in *Carpenter* and *Almonor* stated, the *Katz* test requires courts to analyze the nature of the particular documents, not just the amount of information that they reveal.[276] Thus, even if the amount of CSLI collected only covered a short period of time, it would not change the analysis. This is because, "it is not . . . the length of the monitoring that offends the constitution but rather the place of the monitoring . . . that does."[277]

When law enforcement tracks an individual in real-time, it is doing so blindly. Law enforcement obtains an individual's real-time CSLI "without knowing in advance where or [sometimes] even who they are."[278] This means that law enforcement may ping a cell phone when the individual is in a constitutionally protected place, such as the home. This is true regardless of whether law enforcement tracks a person for three hours, seven days, or several months.

If law enforcement agencies "warrantlessly enter a private home to determine a defendant's location, they cannot successfully justify that invasion of privacy by arguing that they stayed inside for just a short time."[279] With collection of real-time CSLI, the "result should be no different."[280]

C. States Should Pass Legislation Prohibiting the Collection of CSLI

Instead of waiting for the issue to make its way to the Supreme Court, states should take matters into their own hands and pass

274. *Sims*, 569 S.W.3d at 645–46 (explaining that "[w]hether a particular government action constitutes a 'search' or 'seizure' does not turn on the content of the CSLI records; it turns on whether the government searched or seized 'enough' information").

275. Brief of Amici Curiae Electronic Frontier Foundation & American Civil Liberties Union of Massachusetts, Inc. et al., *supra* note 260, at 16.

276. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); Commonwealth v. Almonor, 120 N.E.3d 1183, 1192 n.11 (Mass. 2019).

277. Brief of Amici Curiae Electronic Frontier Foundation & American Civil Liberties Union of Massachusetts, Inc. et al., *supra* note 260, at 15.

278. *Id.* at 19.

279. *Id.* at 14.

280. *Id.*

legislation prohibiting the collection of *all* CSLI without a warrant. Presently, nine states require a warrant to access all CSLI, four states prohibit real-time tracking without a warrant, and two states require a warrant for the use of cell-site simulators.[281] However, this is not enough. All states that do not currently require a warrant to access all CSLI should look to Utah's Electronic Information or Data Privacy Act[282] ("HB 57") as a model.

Utah's HB 57, which was passed on March 27, 2019,[283] is the most protective law concerning third-party-held data and represents a huge step in the right direction.[284] It not only imposes a warrant requirement for *all* location information transmitted by an electronic device, it also "ensures that search engines, email providers, social media, cloud storage, and any other third-party 'electronic communications service' or 'remote computing service' are fully protected under the Fourth Amendment (and its equivalent in the Utah Constitution)."[285] Thus, this law protects even "private electronic data stored with third parties such as Facebook, Dropbox, Twitter, or Google without a warrant."[286] In addition, "once agencies execute a warrant, they must then notify owners within 14 days that their data has been searched"[287] and must "'destroy in an unrecoverable manner' the data it obtains 'as soon as reasonably possible after the electronic information or data is collected.'"[288]

281. *See* LEVINSON-WALDMAN, *supra* note 29, at 4.

282. *See* H.B. 57, 2019 Gen. Sess. (Utah 2019).

283. *See* Cara MacDonald, *Gov. Herbert Signs Bill Requiring Police Obtain Search Warrants to Access Electronic Information*, KSL.COM (Mar. 28, 2019, 6:28 PM), https://www.ksl.com/article/46520524/gov-herbert-signs-bill-requiring-police-obtain-search-warrants-to-access-electronic-information.

284. *See* Nick Sibilla, *Utah Bans Police from Searching Digital Data Without a Warrant, Closes Fourth Amendment Loophole*, FORBES (Apr. 16, 2019, 11:35 AM), https://www.forbes.com/sites/nicksibilla/2019/04/16/utah-bans-police-from-searching-digital-data-without-a-warrant-closes-fourth-amendment-loophole (explaining that "Utah became the first state in the nation to ban warrantless searches of electronic data").

285. *Id.*

286. Anna Parsons, *Utah Has Stepped Up to Protect Fourth Amendment Rights Online. Will Your State Do the Same?*, WASH. EXAMINER (June 19, 2019, 12:00 AM), https://www.washingtonexaminer.com/opinion/op-eds/utah-has-stepped-up-to-protect-fourth-amendment-rights-online-will-your-state-do-the-same.

287. Sibilla, *supra* note 284.

288. Allison Grande, *Utah Warrant Bill Raises Stakes for Cops' Digital Data Grabs*, LAW360 (Apr. 23, 2019, 9:30 PM), https://etron.lls.edu:2195/articles/1151791/utah-warrant-bill-raises-stakes-for-cops-digital-data-grabs.

VI. CONCLUSION

The Fourth Amendment was implemented to protect people from unreasonable searches and seizures. However, the warrantless collection of CSLI disregards that notion. Advances in technology move much faster than the law, so courts must make a concerted effort to keep up. Fortunately, it seems they are doing so. When it comes to the protection of an individual's CSLI, "a consensus appears to be emerging in favor of a warrant requirement."[289] This trend is evidenced by judicial decisions such as *Carpenter* and *Almonor* and legislation such as HB 57. These actions indicate a "broader trend" and effort by judiciaries and legislators to "define the parameters" of digital protection.[290] In effect, these rulings and legislation are chipping away at the third-party doctrine of the 1970s and making it clear that the law must evolve with advancing technology.[291] It looks promising that, in the near future, all Americans will be properly protected against warrantless searches of their CSLI.

289. LEVINSON-WALDMAN, *supra* note 29, at 2.

290. *See* Grande, *supra* note 288 ("This is part of a broader trend that we're seeing in the legislative and judicial arenas to really sort of define the parameters of cyber investigations in terms of what's available to law enforcement and under what standard." (quoting Edward McAndrew, a DLA partner and former federal cybercrime prosecutor)).

291. *See id.* ("As the Supreme Court has said, digital is different, and I think this is a recognition of that, at least by one state." (quoting Edward McAndrew)).