FIND MY FRIENDS: POLICE EDITION— ANALYSIS OF *UNITED STATES V. HAMMOND* AND THE RIGHT TO PRIVACY IN REAL-TIME CSLI

JULIA ZUCHKOV*

INTRODUCTION

When was the last time you left home without your phone? If you are like most Americans, leaving home without your "constant companion" might instill in you a sense of panic, anxiety, or uneasiness.[1] This is not surprising considering our phones serve as our alarm clocks, calendars, wallets, heart rate monitors, restaurant menus,[2] front door keys,[3] and even our way of meeting new love interests. Inadvertently, they also serve as a valuable surveillance tool for law enforcement—one which ninety-seven percent of Americans voluntarily carry.[4] Our cell phones not only store a plethora of personal data but also catalogue virtually all our movements.[5] Regular access to cell phone location information can tell law enforcement whether someone is a heavy drinker, a regular churchgoer, or faithful to their spouse.[6] Not only is law enforcement able to

---

* J.D. Candidate, 2023, Indiana University Robert H. McKinney School of Law; B.A., 2016, University of California–Davis. I would like to extend the utmost gratitude to Professor Yvonne Dutton for her invaluable guidance and for somehow striking the perfect balance between challenging me and encouraging me. I would be remiss if I did not thank the scholarship donors and staff of McKinney Law for allowing me the opportunity to pursue a legal education, which I am immeasurably grateful for. I would also like to thank my family and friends for finding countless typos and reminding me when it is time to take a break.

1. Trevor Wheelwright, *2022 Cell Phone Usage Statistics: How Obsessed Are We?*, REVIEWS.ORG (Jan. 24, 2022), https://www.reviews.org/mobile/cell-phone-addiction/ [https://perma.cc/6TBB-CYNZ].

2. *See* Amelia Lucas, *QR Codes Have Replaced Restaurant Menus. Industry Experts Say It Isn't a Fad*, CNBC (Aug. 21, 2021, 10:30 AM), https://www.cnbc.com/2021/08/21/qr-codes-have-replaced-restaurant-menus-industry-experts-say-it-isnt-a-fad.html [https://perma.cc/QR57-Q22V].

3. *See* Geoffrey A. Fowler, *The Lock Has Evolved: Open Doors With Your Phone*, WALL ST. J. (Oct. 15, 2014, 12:24 PM), https://www.wsj.com/articles/the-lock-has-evolved-open-doors-with-your-phone-1413291632 [https://perma.cc/8UG9-6RMC].

4. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/BP59-BR6B]; *see* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015) ("Most American adults own cell phones, and cell-phone users tend to keep their cell phones close at hand and carry their cell phones with them wherever they go.")

5. Lode, *supra* note 4 ("When a cell phone is turned on, it identifies its location to nearby cell towers, every seven seconds, on a continuous basis.").

6. *Geolocation Technology and Privacy: Hearing on H.R. 2168 Before the H. Comm. on Oversight and Gov't Reform,* 114th Cong. 1 (2016) (statement of Rep. Jason Chaffetz, Chairman, H. Comm. on Oversight and Gov't Reform) [hereinafter *2016 Hearing*].

ascertain such personal details in real-time, but according to a 2021 decision issued by the Seventh Circuit, they may be able to do so without judicial oversight or a probable cause requirement.[7]

Cell phones are constantly attempting to connect to the strongest cell phone tower in their vicinity to ensure the best possible signal.[8] Every time a phone connects to a cell phone tower (typically every seven seconds),[9] cell site location information ("CSLI") is collected and recorded[10] by phone companies.[11] There is no way to circumvent this process short of turning off the cell phone,[12] and—because all cell phones need to connect to a cell phone tower to be operational—even non-smart phones can be tracked.[13]

Phone companies have access to CSLI collected in real-time ("real-time CSLI") and can store real-time CSLI for up to seven years.[14] This stored compilation of real-time CSLI provides a historical record of where a cell phone and its user were located on previous days ("historical CSLI").[15] Law enforcement has the capacity to request both historical and real-time CSLI from cell phone companies when certain conditions are met.[16]

The latest guidance from the Supreme Court requires that law enforcement obtain a search warrant supported by probable cause prior to obtaining a user's historical CSLI.[17] In *Carpenter v. United States*, the Court took issue with law enforcement's ability to escape the practical limits of traditional surveillance[18] and to create a retrospective dossier of an individual's movements.[19] However,

---

7. *See* United States v. Hammond, 996 F.3d 374 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022).

8. *What Is a Cell Tower and How Does a Cell Tower Work?*, MILLMAN LAND (May 12, 2020), https://millmanland.com/company-news/what-is-a-cell-tower-and-how-does-a-cell-tower-work/ [https://perma.cc/U7AZ-NQ5Q].

9. Lode, *supra* note 4 ("When a cell phone is turned on, it identifies its location to nearby cell towers, every seven seconds, on a continuous basis.").

10. Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner at 11, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 4512266 ("Cell providers store this data for up to five years and can also track CSLI in near real-time.") [hereinafter Carpenter Brief].

11. *E.g.,* AT&T, Verizon, MetroPCS, T-Mobile, etc.

12. Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy,* BRENNAN CTR. FOR JUST. 1, 2 (2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Cell_Surveillance_Privacy.pdf [https://perma.cc/5JD3-VVP7].

13. *What Is a Cell Tower and How Does a Cell Tower Work?*, *supra* note 8 ("Whenever a cell phone is used, it emits an electromagnetic radio wave, called a radio frequency, that is received by the nearest cell tower's antenna.").

14. Levinson-Waldman, *supra* note 12, at 2.

15. *Id.* at 3.

16. *Id.* at 4.

17. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

18. *Id.* at 2217-18.

19. *Id.* at 2217.

Carpenter's narrow holding did not extend to the collection of real-time CSLI.[20]

Lower courts have addressed the gap left by *Carpenter* as to real-time CSLI, which has resulted in a split of decisions. Some courts have concluded that real-time CSLI requires a warrant supported by probable cause because the privacy concerns present in the collection of historical CSLI are also present—if not amplified—in the collection of real-time CSLI.[21] But other courts have been hesitant to extend a probable cause warrant requirement to law enforcement's collection of real-time CSLI.[22]

In a matter of first impression, the Seventh Circuit aligned itself with the second set of courts, rejecting the opportunity to extend the probable cause requirement to the collection of real-time CSLI.[23] In 2021, the Seventh Circuit in *United States v. Hammond* held that the short-term collection of real-time CSLI did not constitute a Fourth Amendment search because it did not invade a constitutionally protected area.[24]

This note addresses the gap left by *Carpenter* regarding real-time CSLI and argues that real-time CSLI presents the same privacy concerns as historical CSLI, and thus, necessitates a warrant supported by probable cause. Part I of this note clarifies how cell phones passively track their users' location, how law enforcement compels cell phones to reveal their location using pings, and the legal standard required for such action. Part II explains Fourth Amendment jurisprudence regarding the tracking of criminal suspects as well as Supreme Court precedent that has expanded on what constitutes a search or seizure. Particularly, this section discusses *Carpenter*, where the Supreme Court concluded that law enforcement's collection of historical CSLI constituted a search and required a warrant supported by probable cause. Part III illustrates a split in decisions from lower courts regarding the collection of real-time CSLI. Although some courts have held that the collection of real-time CSLI should require a warrant supported by probable cause, others have held that whether law enforcement conducted a Fourth Amendment search depends on the length and type of data it collected. Part IV discusses *United States v. Hammond*, where the Seventh Circuit held that law enforcement was not required to obtain a warrant supported by probable cause prior to collecting a suspect's real-time CSLI due to the relatively short length of time that the data was collected and the fact that the

---

20. *Id.* at 2220.

21. *E.g.,* State v. Brown, 202 A.3d 1003, 1014, 1018 (Conn. 2019) ("The concerns expressed by the court in *Carpenter* regarding historical CSLI apply with equal force to prospective CSLI."); *see also* Commonwealth v. Almonor, 120 N.E.3d 1183, 1188, 1191 (Mass. 2019) (concluding that a "ping" constitutes a search under the Fourth Amendment).

22. *E.g.,* Andres v. State, 254 So. 3d 283, 297 n.7 (Fla. 2018) ("[W]e conclude that [the *Carpenter*] holding is not applicable . . . where officers used real-time cell-site location information . . . ."); *see also* United States v. Hammond, 996 F.3d 374, 390 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022) ("Real-time CSLI collected over the course of several hours simply does not involve the same level of intrusion as the collection of historical CSLI.").

23. *Hammond*, 996 F.3d 374.

24. *Id.* at 379, 389.

suspect was located on a public road. Part V demonstrates why the approach adopted by the Seventh Circuit is problematic and argues that it inadequately addressed a reasonable expectation of privacy that cell phones users have in their real-time CSLI, failed to account for how ever-evolving technology can invade this right to privacy, and required too tedious of an analysis to offer any meaningful guidance for law enforcement or any meaningful protection for the public. Further, this Part V argues that a federally mandated warrant requirement is the ideal way to adequately balance both law enforcement's need for a uniform standard and society's expectations of privacy in their real-time movements. Although previous attempts at establishing a federally mandated standard have failed,[25] the decisions in *Carpenter* and *Hammond* indicate that this issue is ripe for federal intervention.

I. HOW CELL PHONES WORK & HOW LAW ENFORCEMENT ACCESSES CSLI

A. How Cell Phones Track Your Location

As 97%[26] of Americans go about their days with their phones, their location information is passively collected and stored by phone companies.[27] Cell phone location can be tracked either by global positioning system (GPS) data or CSLI.[28] All cell phones, except for those that have been powered off, automatically search for the closest possible cell tower that would provide the best possible signal and adjust their connection accordingly.[29] For a cell phone "to be usable at all—it must connect with a cell tower."[30] This automated process happens "even in the absence of any user interaction with the phone," and as often as every seven seconds.[31] As users move further from one tower, their phones automatically connect to one of the other 400,000 cell towers in the United States.[32] Because of the growing number of cell phone towers[33] and advancing technology, cell phones are able to triangulate an individual's location with such a high degree of

---

25. *See* Geolocation Privacy and Surveillance ("GPS") Act, H.R. 1062, 115th Congress (2017).

26. *Mobile Fact Sheet*, *supra* note 4.

27. Carpenter Brief, *supra* note 10, at 10 ("When cell phones connect to cell sites, they generate CSLI . . . . Modern cell phones . . . routinely send and receive data whenever the phone is on.").

28. *See generally* Stephanie Lacambra, *Cell Phone Location Tracking or CSLI*, ELEC. FRONTIER FOUND., https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf [https://perma.cc/929Z-AJUC] (last visited Jan. 28, 2022) (GPS tracking relies on a connection with satellites orbiting Earth, whereas CSLI relies on cell phone towers). For purposes of this note, there is no relevant difference between location data that is collected via GPS or CSLI.

29. Carpenter Brief, *supra* note 10, at 6.

30. *Id.* at 2.

31. *Id.* at 11.

32. *Id.*; Thomas Alsop, *Number of Mobile Wireless Cell Sites in the United States from 2000 to 2019,* STATISTA (Sept. 2, 2021), https://www.statista.com/statistics/185854/monthly-number-of-cell-sites-in-the-united-states-since-June-1986/ [https://perma.cc/2FT3-WG6S].

33. *See* Alsop, *supra* note 32.

precision that they can identify "the location of someone inside a building or what floor they're on."[34] The incredibly precise real-time CSLI is passively collected by a user's cell phone company and compiled into a historical record of an individual's movements, in part to aid cell phone companies in improving their user experience. For instance, Google is able to predict the length of trips and traffic patterns by storing user traffic data to analyze trends, and cell phone companies are able to find weak spots in their network and apply roaming charges by tracking location data.[35]

B. How and Why Law Enforcement Accesses CSLI

Law enforcement uses both historical CSLI and real-time CSLI to aid in its investigations. For instance, law enforcement can use historical CSLI to backtrack a suspect's location and determine whether the suspect was present at a specific location at the time of an alleged crime[36] and can use real-time CSLI to locate a suspect so they can execute an arrest[37] or find the suspect again if they have lost visual surveillance.[38]

Real-time CSLI can be tracked either on a prospective basis (the data that is passively collected and stored by users as they connect to cell phone towers) or through "pings," a process where law enforcement requests that cell phone companies "ping" the cell phone causing it to reveal its location.[39] Prospective collection allows law enforcement to monitor a suspect's cell phone and identify its location when it happens to connect to a cell tower on its own, whereas pinging the phone forces it to connect to a cell tower in the moment, allowing law

---

34. Andy Greenberg, *Reminder to Congress: Cops' Cellphone Tracking Can Be Even More Precise Than GPS*, FORBES (May 17, 2012, 1:57 PM), https://www.forbes.com/sites/andygreenberg/2012/05/17/reminder-to-congress-cops-cellphone-tracking-can-be-even-more-precise-than-gps/?sh=1b1ef5ef2184 [https://perma.cc/6W4T-TP3H].

35. *See generally* Emilee Rader, *How Companies Are Using Cell Phone Data*, MSU TODAY (Feb. 11, 2019), https://msutoday.msu.edu/news/2019/how-companies-are-using-cell-phone-data [https://perma.cc/X5UX-X4UT]; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2212 ("Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites. . . . Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.").

36. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2212 (2018).

37. *See, e.g.*, United States v. Hammond, 996 F.3d 374, 390 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022).

38. *See, e.g.*, State v. Muhammad, 451 P.3d 1060, 1067 (Wash. 2019); *see also* United States v. Hammond, 996 F.3d 374, 381 (7th Cir. 2021).

39. Levinson-Waldman, *supra* note 12, at 2 (explaining that "pinging" relies on technology called "Enhanced 911 (E911) data, which allows law enforcement to pinpoint the location of cell phones that have placed 911 calls; a provider can also make a reverse 911 call, allowing the police to invisibly track a target's cell phone in real time.").

enforcement to gauge a suspect's location immediately.[40] Additionally, law enforcement can "circumvent the service provider [altogether] and gain direct access to real-time cell phone location data" using cell site simulators.[41] Rather than pinging a specific cell phone, cell site simulators (also known as "stingrays") are suitcase-sized devices (usually driven around in law enforcement surveillance vehicles) that "'masquerade[] as a cell tower, tricking *all* nearby cell phones to connect to itself' rather than to a legitimate tower."[42]

C. The Standard of Proof Necessary for Law Enforcement to Access CSLI

Real-time and historical CSLI can be accessed by law enforcement if a certain standard of proof is met. Although some documents—such as call records—can be obtained with as little as a subpoena,[43] law enforcement typically must comply with either the "probable cause" standard or the "reasonable grounds" standard to obtain historical or real-time CSLI data records.[44]

The probable cause standard is rooted in the Fourth Amendment and acts somewhat as a "check" on law enforcement. The Fourth Amendment protects against unreasonable searches and seizures by requiring law enforcement to obtain a warrant and comply with four requirements: (1) the warrant must be supported by probable cause; (2) the warrant must particularly describe the place to be searched and persons or things to be seized; (3) the justification for the warrant must be supported by oath or affirmation;[45] and (4) the warrant must be approved by a neutral and detached judicial officer or magistrate.[46] To show probable cause, law enforcement must first gather enough evidence to demonstrate, with a degree of certainty, that a search will lead to evidence of a crime, or a seizure will lead to apprehension of a suspect.[47] The judge or

---

40. *Id.*

41. *Id.*

42. *Id.* (emphasis added) (citation omitted). The subject of this note concerns the collection of real-time CSLI generally; stingrays are one mechanism by which real-time CSLI can be collected. However, stingrays may present additional privacy concerns by virtue of their ability to circumvent the third-party cell phone provider and their ability to collect large amounts of data simultaneously from a group of individuals rather than one suspect. *Id.* This note argues that the general collection of real-time CSLI should require a warrant supported by probable cause, which would encompass the collection of stingray data. This note will not specifically discuss the additional privacy concerns that may be present in the use of stingrays.

43. Lars Daniel, *Cell Phone Records As Evidence in Legal Cases*, ATT'Y AT L. MAG. (Sept. 28, 2017), https://attorneyatlawmagazine.com/cell-phone-records-as-evidence-in-legal-cases [https://perma.cc/64QP-ZDZB]; *see also* FED. R. CRIM. P. 17; 1 CRIM. PRAC. MANUAL § 18:33 (2022) (explaining that information sought with a subpoena must be "relevant" to the investigation—a lesser standard than what is required for a search warrant).

44. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

45. U.S. Const. amend. IV.

46. *See, e.g.*, Shadwick v. City of Tampa, 407 U.S. 345, 349-50 (1972).

47. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 235 (1983).

magistrate then "make[s] a practical, common-sense decision whether, given all the circumstances . . . there is a fair probability that contraband or evidence of a crime will be found."[48] The judge or magistrate also determines the proper scope for the search by ensuring that it satisfies particularity requirements.[49] Generally, if law enforcement conducts a search or seizure without a warrant where a warrant was required, then the action is "presumptively unreasonable"[50] and the prosecution risks not being able to use the evidence at trial to establish the suspect's guilt.[51]

The extensive probable cause process protects the public from arbitrary government intrusion.[52] However, because it can be time-consuming to fulfill the requirements, the Fourth Amendment also allows for exceptions.[53] One such exception is the existence of an exigent circumstance, which permits officers to conduct a search or seizure without first obtaining a warrant in emergency situations (i.e., exigent circumstances) where there is probable cause to believe that a search or seizure is necessary.[54] An exigent circumstance exists when a reasonable officer would believe that the search or seizure is necessary to prevent harm to officers or civilians, necessary to prevent the destruction of evidence, or necessary to prevent the escape of a suspect.[55] For instance, if law enforcement are in hot pursuit of an active shooter who runs into a home, law enforcement are not required to stop outside the home and obtain a warrant prior to entering, so long as they have probable cause to believe that the suspect is in fact the shooter and did in fact run into the home.

---

48. *Id.* at 238.

49. *See, e.g.*, Marron v. U.S., 275 U.S. 192, 195-96 (1927) (explaining that courts of the United States are responsible for ensuring particularity in search warrants and that "nothing is left to the discretion of the officer executing the warrant.").

50. Groh v. Ramirez, 540 U.S. 551, 559 (2004).

51. *See* Mapp v. Ohio, 367 U.S. 643, 657 (1961) (holding that "the exclusionary rule is an essential part of both the Fourth and Fourteenth Amendments [and] is not only the logical dictate of prior cases, but it also makes very good sense").

52. Camara v. Mun. Ct. of City and Cnty. of San Francisco, 387 U.S. 523, 528 (1967) (stating that the purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government" actors).

53. *See generally Exceptions to the Warrant Requirement,* LAWSHELF EDUC. MEDIA (last visited Feb. 25, 2022), https://lawshelf.com/coursewarecontentview/exceptions-to-the-warrant-requirement [https://perma.cc/3BSM-MVWX] (Exigent circumstances are discussed here due to their relevance in *United States v. Hammond*, 996 F.3d 374, 390 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022) (*see infra* text accompanying notes 176-82)).

54. *Id.* Other exceptions to the warrant requirement include the plain view doctrine, the automobile exception, searches incident to a lawful arrest, consent, stop & frisk, and protective sweeps. *Id.*

55. *See* Kentucky v. King, 563 U.S. 452, 460 (2011); *see also* Michigan v. Fisher, 558 U.S. 45, 47 (2009) (to render emergency assistance to an injured occupant); *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("to prevent the imminent destruction of evidence"); *see also* United States v. Santana, 427 U.S. 38, 42-43 (1976) (when in hot pursuit of a fleeing suspect).

Further, the Supreme Court has instructed that some lesser intrusions require only a lower *reasonable grounds* standard.[56] This standard does not require pre-approval by a judge or magistrate, does not need to fulfill particularity or specificity requirements, does not need to fulfill probable cause requirements, and does not need to be supported by oath or affirmation.[57] To fulfill the reasonable grounds standard, law enforcement must show only that they believed the public was in danger and that it limited the scope of its search or seizure to limit that danger.[58] For instance, when law enforcement conducts a "stop and frisk" of a suspect to check for weapons, a law enforcement officer is merely required to demonstrate that they had reasonable grounds to believe that the public was in danger and that they limited the scope of their pat down to search for weapons.[59]

Identifying which standard of proof applies to law enforcement's collection of real-time CSLI will inform whether law enforcement must comply with the probable cause requirements outlined by the Fourth Amendment. However, there is currently no federal legislation or Supreme Court precedent addressing this issue.

II. FOURTH AMENDMENT AND SUPREME COURT PRECEDENT

The Supreme Court has not directly addressed whether law enforcement's collection of real-time CSLI constitutes a search; however, it has held that law enforcement must obtain a warrant supported by probable cause prior to collecting historical CSLI.[60] An examination of existing Fourth Amendment precedent and an analysis of *Carpenter* supports the argument that real-time CSLI should also require a search warrant supported by probable cause.

Determining whether governmental action should be subject to Fourth Amendment protection merits an evaluation of an individual's reasonable expectation of privacy.[61] The Fourth Amendment protects "people, not places"[62] and does not turn only on whether law enforcement physically invades a private area.[63] The reasonable expectation of privacy test, also known as the *Katz* test, outlines that governmental action constitutes a search if an individual maintains an actual, subjective expectation of privacy (i.e., whether they took any affirmative action that indicates their expectation of privacy) and whether this expectation is one society is prepared to deem reasonable (i.e., whether other members of the public similarly believe that such action warrants an expectation

---

56. Terry v. Ohio, 392 U.S. 1, 30 (1968).

57. *Id.* at 38 (Douglas, J., dissenting).

58. *Id.* at 30.

59. *Id.* at 29-30.

60. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018). ("Government must generally obtain a warrant supported by probable cause before acquiring [CSLI from a wireless carrier].").

61. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

62. *Id.* at 351.

63. *Id.* at 353 ("[T]he 'trespass' doctrine . . . can no longer be regarded as controlling.").

of privacy).[64]

Traditionally, the Supreme Court relied on the common law concept of trespass in determining whether the government's conduct was unreasonable such that it should have first obtained a warrant supported by probable cause.[65] In some early cases, the Court held that individuals have a diminished expectation of privacy when they are in a public location as opposed to a private locale.[66] For instance, in *United States v. Knotts,* officers placed a tracking device into a chloroform container purchased by a suspect then followed the suspect's vehicle as he drove the chloroform to his cabin.[67] The Court held that this type of tracking did not invade the driver's privacy rights because drivers have "no reasonable expectation of privacy" on public thoroughfares.[68] As such, the Court held that the government acted properly in not obtaining a warrant prior to tracking the suspect's movements on public roads because "there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment."[69]

The Court has disagreed on whether to apply a *Katz* test or to base its reasoning solely on whether law enforcement physically intruded onto private property. Illustrative is *United States v. Jones*, where officers placed a tracking device on a suspect's vehicle and used it to track his movements for twenty-eight days.[70] Although a unanimous Court agreed that the government conducted a Fourth Amendment search and was first required to obtain a warrant supported by probable cause, the Justices advocated different reasons for their conclusions.[71] The majority reasoned that law enforcement violated the Fourth Amendment because they trespassed onto the suspect's private property to place the GPS tracker onto the vehicle in the first place.[72] However, four concurring justices, led by Justice Alito, advocated for an application of the *Katz* test rather than a reliance on the majority's common law trespass.[73] Justice Alito and Justice Sotomayor wrote separate concurrences but both similarly forecasted that future cases would need to deal with the difficult question of electronic monitoring, which will permit law enforcement to remotely conduct a search and track an individual's location without having to physically trespass onto their property.[74]

---

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

65. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled by Katz,* 389 U.S. 347.

66. *See* United States v. Knotts, 460 U.S. 276 (1983).

67. *Id.* at 278.

68. *Id.* at 281.

69. *Id.* at 285.

70. 565 U.S. 400, 403 (2012).

71. *See id.* at 411-31.

72. *Id.* at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

73. *Id.* at 419 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated . . . .").

74. *Id.* at 427 (Alito, J., concurring) ("[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations."); *id.* at 415 (Sotomayor, J., concurring) ("GPS

A. Reasonable Expectation of Privacy in Historical CSLI

The most significant Fourth Amendment case to reach the Supreme Court since *Jones*[75] is *Carpenter*, where the Court addressed whether the government's warrantless collection of historical CSLI violated the Fourth Amendment.[76]

In *Carpenter,* officers arrested four suspects in a series of robberies which had taken place over several months.[77] One of the suspects confessed to the robberies, identified his accomplices, and provided law enforcement with their phone numbers.[78] Prosecutors applied for a court order pursuant to the Stored Communication Act ("SCA") requiring the disclosure of historical CSLI data from the dates of the robberies for Carpenter and several other suspects.[79] The SCA—passed by Congress in 1986—requires only "*reasonable grounds* to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[80] In compliance with this standard, magistrate judges approved two orders, and the government ultimately obtained "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[81] The officers used this retrospective information to confirm that Carpenter was present at the site of the robberies at the time the robberies occurred.[82] Based on the data, "Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence."[83]

Carpenter brought a motion to suppress the historical CSLI, arguing that the government's collection of these records violated the Fourth Amendment because law enforcement relied on the lesser reasonable grounds standard rather than obtaining a warrant supported by probable cause.[84] The Government argued that the third-party doctrine should rule here, meaning that because Carpenter voluntarily provided his cell phone company with his location data, he did not maintain a reasonable expectation of privacy in these records.[85] The Supreme Court ultimately sided with Carpenter, holding that the Government was required to obtain a warrant supported by probable cause prior to obtaining Carpenter's historical CSLI.[86] The Court reasoned that individuals maintain a reasonable

---

monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

75. 565 U.S. 400 (2012).
76. Carpenter v. United States, 138 S. Ct. 2206 (2018).
77. *Id.* at 2212.
78. *Id.*
79. *Id.*
80. 18 U.S.C. § 2703(d) (emphasis added).
81. *Carpenter*, 138 S. Ct. at 2212.
82. *Id.* at 2213.
83. *Id.* at 2212.
84. *Id.*
85. *Id.* at 2219.
86. *Id.* at 2221.

expectation of privacy in their historical CSLI, and that they do not waive this right to privacy merely because the cell phone company maintains these records.[87]

The Court used the *Katz* test to analyze whether Carpenter had a reasonable expectation of privacy in a record of his physical movements.[88] Although the Court identified past precedent indicating that there is a diminished expectation of privacy on public roads, it concluded that this past precedent did not necessarily apply to modern technology that would allow for "twenty-four hour surveillance of any citizen of this country."[89] The Court took issue with law enforcement's unfettered access to a device that travels far beyond public roads, "follow[ing] its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[90] Prior to the pervasiveness of modern technology, law enforcement did not have the resources to follow one suspect for long stretches of time and catalogue all their movements.[91] Today individuals carry their cell phones with them everywhere, thus allowing the government continuous access to a cell phone's location is akin to attaching an ankle monitor to a cell phone's user.[92]

The Court then addressed whether a person waives this expectation of privacy by sharing location information with cell phone companies and voluntarily carrying a cell phone.[93] Precedent has applied this idea, known as the third-party doctrine, to dialed telephone numbers and bank records holding that individuals voluntarily assume the risk that these records will be divulged to law enforcement.[94] However, the Court declined to extend the third-party doctrine to historical CSLI collected by cell phone companies.[95] Instead, the Court found that applying the third-party doctrine to CSLI would fail to address "the seismic shifts in digital technology" that allow for long-term tracking of practically anyone.[96] The Court held that disclosure of these records to a third-party cell phone company does not overcome an individual's expectation of privacy in the whole of their physical movements.[97] Further, it held that individuals do not waive their right to privacy because there is no affirmative waiver on the part of the cell

---

87. *Id.* at 2222.

88. *Id.* at 2217.

89. *Id.* at 2215 (quoting United States v. Knotts, 460 U.S. 276, 283-84 (1983)).

90. *Id.* at 2218.

91. *Id.* at 2217. The *Carpenter* Court recognized "society's expectation . . . that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

92. *Id.* at 2218.

93. *Id.* at 2216.

94. *Id.* at 2216 (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

95. *Id.* at 2217.

96. *Id.* at 2219.

97. *Id.*

phone user.[98] In fact, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[99]

Further, the Court took issue with the nature of historical CSLI allowing for a retrospective cataloguing of an individual's movements, allowing officers to recreate past records in a way they otherwise would not be able to.[100] Unlike a GPS tracker, which law enforcement installs once an individual becomes a suspect in a crime, historical CSLI is collected from everyone with a cell phone, long before they are identified as suspects.[101] Accordingly, the Court said that "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day . . . and the police may . . . call upon the results of that surveillance without regard to the constraints of the Fourth Amendment."[102] Allowing the government this breadth of access means that only those without cell phones—an ever shrinking minority—would "escape this tireless and absolute surveillance."[103]

Although the Court specified that its narrow holding does not apply to the collection of real-time CSLI, it held that individuals have a "legitimate expectation of privacy in the record of [their] physical movements as captured through [historical] CSLI."[104] The dissent took issue with, among other things, the majority's failure to indicate just how much information must be requested by law enforcement to trigger a warrant requirement.[105] Indeed, Justice Gorsuch, dissenting, took issue with the majority's limited analysis regarding real-time CSLI.[106] Namely, he questioned "*what* distinguishes historical data from real-time data" and rightly predicted that the majority opinion "raises more questions for lower courts to sort out."[107]

III. SPLIT IN AUTHORITY

Lower court decisions have split into two camps as they grapple with the gap left by *Carpenter* regarding real-time CSLI. The first camp maintains that the privacy concerns articulated by the Supreme Court in *Carpenter* as they relate to historical CSLI are emulated—if not amplified—by the warrantless collection of real-time CSLI. These courts have concluded that the collection of real-time CSLI constitutes a Fourth Amendment search and requires a warrant supported by probable cause.[108] Conversely, the second camp concludes that individuals do not

98. *Id.* at 2220.
99. *Id.*
100. *Id.* at 2218.
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.* at 2217.
105. *Id.* at 2266-67 (Gorsuch, J., dissenting).
106. *Id.* at 2666 (Gorsuch, J., dissenting).
107. *Id.* at 2267 (Gorsuch, J., dissenting) (emphasis added).
108. *See* State v. Brown, 202 A.3d 1003, 1018 (Conn. 2019) ("The concerns expressed by the

maintain a legitimate expectation of privacy in their real-time CSLI unless the collection of data exceeds a certain threshold (i.e., the data is collected for too long or extends to a constitutionally protected area).[109]

This split is further illustrated by a concept known as the Mosaic Theory, which evaluates "whether the type and amount of information gathered [by a governmental investigation], when viewed in the aggregate, is so revealing that the action should be considered a Fourth Amendment search."[110] Alternatively, the traditional approach is binary, categorizing each governmental action as either a search or not a search.[111] While the second camp of courts ("mosaic courts") would apply the mosaic theory and evaluate whether law enforcement's collection of real-time CSLI seized *enough* information about the suspect to qualify as an intrusion on their privacy, the first camp of courts ("binary courts") would apply a binary approach and classify the collection of real-time CSLI as a search regardless of the amount of information seized. Below, this note illustrates this split in greater detail.

A. Collection of Real-Time CSLI Is a Search

The Supreme Court of Pennsylvania, Supreme Court of Washington, and Supreme Court of Connecticut make up the binary side of the split.[112] These

---

court in *Carpenter* regarding historical CSLI apply with equal force to prospective CSLI."); *see also* Commonwealth v. Almonor, 120 N.E.3d 1183, 1191 (Mass. 2019) (holding that a "ping" constitutes a search); Commonwealth v. Pacheco, 263 A.3d 626, 641 (Pa. 2021) (holding that individuals have "a legitimate expectation of privacy in [their] continuous real-time CSLI"); State v. Muhammad, 451 P.3d 1060, 1092 (Wash. 2019) (holding that a "ping" is a Fourth Amendment search and "must be supported by a warrant"); Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (a pre-*Carpenter* case where the Supreme Court of Florida held that individuals maintain a "subjective expectation of privacy [in their real-time CSLI]—even on public roads—[and that this] is an expectation of privacy that society is now prepared to recognize as reasonable").

109. *See* United States v. Hammond, 996 F.3d 374, 389-90 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022) ("Real-time CSLI collected over the course of several hours simply does not involve the same level of intrusion as the collection of historical CSLI."); *see also* Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App.), *cert. denied*, 139 S. Ct. 2749 (2019) (holding that there was no legitimate expectation of privacy in "physical movements . . . as reflected in less than three hours of real-time CSLI records accessed by police by pinging [a] phone less than five times"); United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017), *cert. denied*, 138. S. Ct. 2705 (2018) (holding that "the government did not conduct a search under the Fourth Amendment when it tracked" real-time CSLI for approximately seven hours).

110. Robert Fairbanks, Note, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpente*r, 26 BERKELEY J. CRIM. L. 71, 74 (2021).

111. *Id.*

112. *See Pacheco*, 263 A.3d 626; *Muhammad*, 451 P.3d 1060; *Brown*, 202 A.3d 1003; *Almonor*, 120 N.E.3d 1183; *see also Tracey*, 152 So. 3d at 526 (The Supreme Court of Florida has also held that the collection of real-time CSLI constitutes a search pursuant to the Fourth Amendment, but because this case was decided pre-*Carpenter*, it is not characterized as being part of the split illustrated in this

courts hold that cell phone users have a reasonable expectation of privacy in their real-time CSLI.[113] Particularly, the binary courts take issue with real-time CSLI—like historical CSLI—providing law enforcement with a concerning ability to peer into the intimate lives of individuals and secretly catalogue their movements with minimal effort.[114] These courts hold that failing to require a warrant would allow law enforcement to escape judicial oversight or practical limitations (such as cost or efficiency).[115] These courts further hold that individuals do not waive their privacy expectations simply by owning and using a cell phone.[116]

1. Cell Phone Users Have a Reasonable Expectation That They Will Not Be Secretly Monitored and Catalogued.—Although the *Carpenter* Court limited its holding to historical CSLI, the binary courts have extended a reasonable expectation of privacy to law enforcement's collection of real-time CSLI as well.[117] Illustrative is *Pacheco*, where the Supreme Court of Pennsylvania found that the collection of 108 days of real-time CSLI constitutes a Fourth Amendment search and implicates the same privacy concerns that the Supreme Court addressed in *Carpenter*.[118] The court compared this long-term mapping of real-time CSLI to the historical CSLI seen in *Carpenter*, holding that the collection of real-time CSLI similarly provided law enforcement with a window into the cell phone user's personal life and patterns.[119] The court took issue with law enforcement's ability to create a "comprehensive chronicle" of a cell phone user's movements throughout the course of a "lengthy criminal investigation."[120] Further, this novel surveillance technique did not exist prior to the "cell phone age," making it unreasonable for society to expect that law enforcement will be able to "secretly manipulate" cell phones to achieve such thorough and invasive surveillance.[121]

2. Technological Advancements Remove Check on Law Enforcement Action.—Indeed, these courts have also expressed concern with law enforcement replacing traditional visual surveillance with real-time CSLI tracking because it removes the practical check on law enforcement action that used to exist.[122] For

---

note.).

113. *See Pacheco*, 263 A.3d at 641, 652; *Muhammad*, 451 P.3d at 1069; *Brown*, 202 A.3d at 1017-18.

114. *See, e.g.*, *Pacheco*, 263 A.3d at 641.

115. *See, e.g.*, Commonwealth v. Almonor, 120 N.E.3d 1183, 1195 (Mass. 2019) (citing United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring); *id.* at 415-16 (Sotomayor, J., concurring)).

116. *See, e.g.*, *Muhammad*, 451 P.3d at 1072-74.

117. *See, e.g.*, *Pacheco*, 263 A.3d at 635.

118. *Id.* at 640-41.

119. *Id.* at 640 ("[T]he acquisition of 108 days of his real-time CSLI implicates the same privacy concerns that arose from the government's acquisition of continual historical CSLI in Carpenter.").

120. *Id.* at 641.

121. *Id.*

122. State v. Muhammad, 451 P.3d 1060, 1072 (Wash. 2019) (citing United States v. Jones, 565

instance, officers ceased surveillance of a suspect in *Muhammad* for "reasons unknown" and later pinged his phone without a warrant to relocate him.[123] The *Muhammad* court took issue with law enforcement's ability to use pinging as a complete substitute to traditional surveillance.[124] Particularly concerning is that this alternative to traditional surveillance is cheap, easy, and efficient.[125] In the past, protections to privacy were not only constitutional or statutory—but also established by practical limits.[126] Law enforcement simply did not have the resources to conduct long-term surveillance of every suspect in every crime.[127] To conduct even potentially comparable surveillance to what is possible with real-time CSLI would have required a team of officers, multiple vehicles, and potentially aerial surveillance.[128] However, low-cost technology has essentially removed practical limitations on easily-abused law enforcement practices.[129] The collection of real-time CSLI not only allows officers to evade the high costs of such surveillance, but also allows them to invade into constitutionally protected areas that they would not have been able to enter with traditional surveillance without first obtaining a warrant supported by probable cause.

3. Cell Phone Users Do Not Waive Their Right to Privacy.—Courts have further held that individuals do not waive their expectation of privacy by virtue of owning a cell phone and sharing their location with their cell phone company.[130] As identified by the Court in *Carpenter*, there is no way to avoid sharing CSLI unless a user completely turns off their cell phone or disconnects from the network.[131] The *Muhammad* court extended this rationale to the collection of real-time CSLI, holding that individuals maintain an expectation of privacy in their private movements as collected by real-time CSLI and urging courts to consider the "substantial monitoring and tracking capabilities of technology" in determining whether a reasonable expectation of privacy exists.[132] The *Almonor* court specified that an individual's decision to own a cell phone does not permit officers to "independently, and without judicial oversight" manipulate phones to reveal private information.[133]

Because cell phones have become indispensable to a large portion of the population, users do not voluntarily waive their right to privacy by allowing their

---

U.S. 400, 416 (2012) (Sotomayor, J., concurring)).

123. *Id.* at 1067.

124. *Id.* at 1069.

125. *Id.* at 1071-72.

126. Commonwealth v. Almonor, 120 N.E.3d 1183, 1195 (citing *Jones*, 565 U.S. at 415-16 (Sotomayor, J., concurring)).

127. *See Jones*, 565 U.S. at 430 (Alito, J., concurring).

128. *Id.* at 429 (Alito, J., concurring).

129. Tracey v. State, 152 So. 3d 504, 519 (citing *Jones*, 565 U.S. at 415-16 (Sotomayor, J., concurring)).

130. *See, e.g.*, State v. Muhammad, 451 P.3d 1060, 1072-74 (Wash. 2019).

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

132. *Muhammad*, 451 P.3d at 1072.

133. Commonwealth v. Almonor, 120 N.E.3d 1183, 1194 (Mass. 2019).

cell phone company access to their location.[134] Carrying a cell phone all day has practically become a requirement of participating in modern society.[135] Although users may allow their cell phone company to access their location for purposes of call routing, navigation, or weather reporting, this does not translate to a voluntary waiver for law enforcement to track them in real-time at any moment, in any location.[136]

4. Pings Constitute a Search.—The binary courts further believe that the government conducts an intrusion the moment that law enforcement pings a cell phone, compelling it to emit a signal revealing its location, without judicial oversight or an exigency exception.[137] In other words, pinging—on its own—constitutes a Fourth Amendment search.[138] Although historical CSLI is passively collected by cell phone companies, real-time CSLI is collected at the behest of law enforcement.[139] The act of pinging a phone is both initiated and controlled by law enforcement.[140] Allowing law enforcement to secretly manipulate cell phones for any purpose, let alone for the purpose of transmitting private, personal location data for any individual at any time, constitutes an unreasonable infringement into privacy rights.[141]

Courts have also maintained that failing to categorize the initial ping as a search will lead to a practical line-drawing problem. Basing the determination of whether a Fourth Amendment violation has occurred on the length of time that a cell phone is monitored "is not a workable analysis"[142] and this ad hoc determination "offers little guidance to courts or law enforcement."[143] The *Muhammad* court warns that this kind of case-by-case, after-the fact analysis will lead to arbitrary and inequitable enforcement.[144]

B. Collection of Real-Time CSLI Is Not a Search

However, the mosaic courts are not convinced that real-time CSLI constitutes a search. The Texas Court of Criminal Appeals and Seventh Circuit disagree that a ping—on its own—constitutes a search and instead hold that individuals do not maintain a reasonable expectation of privacy in their real-time CSLI unless the breadth of the search extends for too long a period or reveals intimate details from

---

134. *Tracey*, 152 So. 3d at 522.

135. *Almonor*, 120 N.E.3d at 1194 (citing *Carpenter*, 138 S. Ct. at 2220).

136. *Tracey*, 152 So. 3d at 522 ("While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction.").

137. *Muhammad*, 451 P.3d at 1074; *Almonor*, 120 N.E.3d at 1193.

138. *Muhammad*, 451 P.3d at 1074.

139. *Almonor*, 120 N.E.3d at 1193.

140. *Id.*

141. *Id.* at 1193-94.

142. *Tracey*, 152 So. 3d at 520.

143. *Muhammad*, 451 P.3d at 1073.

144. *Id.* (citing Oliver v. United States, 466 U.S. 170, 181-82 (1984)).

a constitutionally protected area.[145]

1. Pings Do Not Automatically Constitute a Search.—The mosaic courts hold that a privacy intrusion does not automatically occur at the ping, but instead requires a case-by-case analysis of whether law enforcement collected too much data or a particularly sensitive type of data.[146] For instance, in *Sims v. State*, the Texas Court of Criminal Appeals held that pinging a suspect's phone less than five times and tracking him for less than three hours did not constitute a search.[147] In *Sims*, officers were investigating a murder and robbery that took place several hours earlier.[148] The victim's family had identified a potential suspect and officers requested—prior to obtaining a search warrant—that the suspect's cell phone company ping his cell phone.[149] Law enforcement tracked the suspect's real-time CSLI for approximately three hours, ultimately finding him near a truck stop.[150] Although the court accepted that the third-party doctrine does not protect the collection of real-time CSLI pursuant to *Carpenter*, it ultimately held that the question of whether a search or seizure occurred turns on whether the government searched or seized enough information.[151]

2. Constitutionally Protected Areas.—In addition to the length of time being relevant to the mosaic courts' analysis, the courts also analyze whether the cell phone user was in a constitutionally protected area when they were pinged. Namely, these courts rely on the diminished expectation of privacy that the Supreme Court held individuals have on public roads in *Knotts*.[152] For instance, in *Riley,* the Sixth Circuit held that a robbery suspect did not have a reasonable expectation of privacy in his real-time CSLI when he was tracked to a motel.[153] The court reasoned that because law enforcement was unable to locate the suspect in the exact motel room without first consulting with the motel's front desk, that law enforcement's real-time tracking did not provide greater insights into his whereabouts than what he voluntarily exposed to public view.[154] Although the Supreme Court has held that the Fourth Amendment draws "a firm line at the entrance to the house,"[155] entitling an individual's residence to the highest

---

145. Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App.), *cert. denied*, 139 S. Ct. 2749 (2019); United States v. Hammond, 996 F.3d 374, 389-90 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022); *see also* United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017), *cert. denied*, 138 S. Ct. 2705 (2018) (holding that several hours of tracking does not constitute a search pursuant to the Fourth Amendment).

146. *Sims*, 569 S.W.3d at 646; *Hammond*, 996 F.3d at 391-92.

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

148. *Id.* at 638.

149. *Id.*

150. *Id.* at 639.

151. *Id.* at 645-46.

152. *E.g.*, United States v. Hammond, 996 F.3d 374, 389 (2021), *cert. denied*, 142 S. Ct. 2646 (2022); United States v. Knotts, 460 U.S. 276, 281 (1983).

153. 858 F.3d 1012, 1013 (6th Cir. 2017).

154. *Id.* at 1018.

155. Payton v. New York, 445 U.S. 573, 590 (1980).

expectation of privacy, the Sixth Circuit found that this "sacred threshold" was not crossed in *Riley* because the real-time CSLI revealed only that the suspect was at this motel, but not in which room.[156]

However, perhaps indicating some disagreement, lower courts applying the mosaic theory continue to maintain that individuals *do* have an expectation of privacy in their homes. The United States District Court for the Middle District of Pennsylvania in *United States v. Baker* found that a suspect had a reasonable expectation of privacy in his real-time CSLI when a ping showed the suspect was within fourteen meters of a home.[157] Officers were investigating a drug deal that had resulted in the buyer being seriously injured by the seller.[158] Officers acquired a search warrant for the house, found the suspects within the house, saw narcotics in plain view, and arrested the defendants.[159] The defendants moved to suppress the narcotics evidence that resulted from the search, arguing that a search warrant was required "prior to conducting the ping to determine [their] real-time location."[160] The court agreed that law enforcement conducted a search when they tracked the suspect's location in a private home because an individual's "presence inside of a particular home is generally considered private, and society does not expect law enforcement to possess the capability of instantaneously locating citizens in private spaces."[161]

IV. *UNITED STATES V. HAMMOND*

In a 2021 decision, the Seventh Circuit adopted the mosaic approach, holding—in a matter of first impression—that law enforcement's short-term warrantless collection of real-time CSLI did not generate enough information to constitute a search.[162]

A. The Facts

In October 2017, a series of robberies occurred in northern Indiana (Logansport, Peru, and Auburn) and southern Michigan (Portage and Kalamazoo).[163] Witnesses from the robberies reported a suspect that wore similar clothes, looked similar in appearance, took similar actions, and carried a tan handgun.[164] Based on the reported similarities and a review of surveillance video,

---

156. *Riley*, 858 F.3d at 1018.

157. United States v. Baker, 563 F. Supp. 3d 361, 379-80 (M.D. Pa. 2021).

158. *Id.* at 368.

159. *Id.* at 369.

160. *Id.* at 367, 375.

161. *Id.* at 381. Denying the motion to suppress, the court specified that the search was presumptively unreasonable and that the warrantless ping may have led to suppression had there not been an exigency exception. *Id.* at 382.

162. United States v. Hammond, 996 F.3d 374, 391-92 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022).

163. *Id.* at 379-80.

164. *Id.* at 380.

a task force comprised of federal and state officers concluded that the same suspect was responsible for all of the robberies and identified a light-colored vehicle they believed to be the getaway car.[165] On October 10, during a robbery in Kalamazoo, the suspect fled the scene without his gun.[166] Law enforcement traced the serial number of the gun to its last federally-licensed dealer and, on October 28, officers discovered that the gun had been sold to a man named Rex for whom they were given a phone number.[167] Officers learned that the number was assigned to Rex Hammond and used Department of Motor Vehicle records to match his vehicle to those of their suspect.[168]

On October 30, a Kalamazoo Police Detective submitted an exigency request to AT&T requesting that AT&T "ping" Hammond's phone and provide his real-time CSLI.[169] The exigent circumstance reported was that "the robber had been entering places of business with his finger on or just adjacent to the trigger of a handgun, had handled the handgun unsafely . . . when he laid it on the counter, and had committed an armed robbery two days before and two days before that, suggesting the next armed robbery might be imminent."[170] AT&T began to "ping" Hammond's phone at 6:00 p.m., reporting the phone's location every fifteen minutes.[171] The Kalamazoo detective notified Indiana State Police that the pings showed Hammond was "first in, then moving away from, Elkhart."[172] Officers left "in unmarked vehicles to track Mr. Hammond's phone" and eventually saw his car and pursued it.[173] After pursuing Hammond's car for approximately thirty-five miles, officers radioed "that they had lost Mr. Hammond."[174]

Later that same evening, a Marshall County Police Officer reported seeing Hammond's car and stopped him.[175] Officers found a gun, mask, grocery bags (allegedly used to collect the money at the robberies), and "other items of evidentiary value" in the vehicle.[176] A Logansport Police Detective arrived on the scene after "traveling toward the reported pings" and told the officers on scene that the county prosecutor "had issued an arrest on sight order" for Hammond.[177] Hammond was taken to jail and the Logansport Detective "arrived the next day with an arrest warrant for . . . the two Logansport robberies."[178]

---

165. *Id.*

166. *Id.*

167. *Id.*

168. *Id.*

169. *Id.* at 381.

170. United States v. Hammond, 3:18-CR-5 RLM-MGG, 2018 WL 5292223, at *2 (N.D. Ind. Oct. 24, 2018), *aff'd*, United States v. Hammond, 996 F.3d 374 (7th Cir. 2021).

171. *Hammond*, 996 F.3d at 381.

172. *Hammond*, 2018 WL 5292223, at *2.

173. *Id.*

174. *Id.*

175. *Hammond*, 996 F.3d at 381.

176. *Hammond*, 2018 WL 5292223, at *2.

177. *Id.*

178. *Id.*

B. United States District Court for the Northern District of Indiana

Hammond moved to suppress all evidence obtained from his vehicle because law enforcement did not obtain a search warrant prior to collecting his real-time CSLI and because there was no exigent circumstance to the warrant requirement.[179] Hammond argued that the *Carpenter* holding extended to real-time CSLI and required law enforcement to obtain a search warrant supported by probable cause prior to pinging and tracking him.[180] The district court believed the government had conceded[181] that *Carpenter's* holding applied in equal force to the collection of real-time CSLI and that law enforcement was therefore required to obtain a search warrant prior to accessing the ping information.[182] However, the district court still denied the motion to suppress due to an exigency exception and in reliance on the good faith exception.[183]

Hammond argued that there was no exigent circumstance because law enforcement had plenty of time to obtain a warrant prior to pinging his phone.[184] However, the district court held that there was an exigency because law enforcement reasonably thought that if they did not locate Hammond as soon as possible, he would commit another robbery with a firearm, endangering the public.[185]

C. United States Court of Appeals for the Seventh Circuit

Hammond appealed the district court's decision to the Seventh Circuit Court of Appeals, again arguing that law enforcement's collection of real-time CSLI constituted a search.[186] On appeal, the Seventh Circuit did not discuss whether an exigency truly existed; instead the court held that Hammond did not have a reasonable expectation of privacy in his real-time CSLI to begin with.[187] The Seventh Circuit clarified that the district court was mistaken in its understanding

---

179. *Id* at *2-3.

180. *Id.* at *3.

181. *But see* United States v. Hammond, 996 F.3d 374, 387 n.4 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022) (clarifying the government did not concede this point but had merely accepted it for the sake of argument).

182. *Hammond*, 2018 WL 5292223, at *2.

183. *Id.* at *4. Neither the exigency nor good faith exception are the subject of this note.

184. *Id.* at *3. Because exigencies are not the subject of this note, this note will not analyze whether an exigency truly existed. However, it is worth noting that several days passed from when law enforcement obtained Hammond's phone number (Oct. 28) to when they warrantlessly requested a ping (Oct. 30). *Id.* at *1-2. As discussed above, exigent circumstances typically require an *immediate* emergency. *See generally* United States v. McConney, 728 F.2d 1195, 1205 (9th Cir.), *cert. denied*, 469 U.S. 824 (1984). Here, law enforcement sat on Hammond's phone number for several days prior to pinging it and likely had enough time to obtain a warrant in the interim.

185. *Hammond*, 2018 WL 5292223, at *3.

186. *Hammond*, 996 F.3d at 382-83.

187. *Id.* at 391-92.

that the government conceded that a warrant was required for the collection of real-time CSLI.[188] In ultimately deciding that real-time CSLI does not constitute a search, the Seventh Circuit focused its discussion on determining whether the facts were more similar to *Carpenter* or *Knotts*.[189]

First, the Seventh Circuit held that because the monitoring in *Hammond* only lasted a matter of hours, it was more similar to the discrete trip in *Knotts* than the 127 days of historical data collected by officers in *Carpenter*.[190] Second, because Hammond was exclusively traveling on public roads when he was tracked, the Seventh Circuit held that the tracking was more similar to *Knotts* than *Carpenter* because there was no data that revealed an "intimate window" into Hammond's life.[191] Third, the Seventh Circuit differentiated between historical and real-time data collection by highlighting the *Carpenter* Court's concern with the "retrospective quality" of historical CSLI.[192] Because this retrospectivity is not present in real-time CSLI, the Seventh Circuit held that the collection of real-time CSLI is less intrusive than the collection of historical CSLI and more similar to the beeper in *Knotts*, particularly because of law enforcement's ability to use historical CSLI to reconstruct a suspect's movements.[193] Fourth, the Seventh Circuit held that society is not prepared to recognize a reasonable expectation of privacy in real-time CSLI.[194] Although the *Carpenter* decision recognized that collection of historical CSLI "contravened society's expectations . . . of law enforcement's capabilities"[195] the Seventh Circuit held that "society is fully aware that officers may follow and track a suspect's movements for several hours" and that "law enforcement's ability to locate Hammond on public roads . . . is not inconsistent with society's expectation of privacy from law enforcement's prying eyes."[196]

V. WHY REAL-TIME CSLI AND HISTORICAL CSLI SHOULD BE TREATED AS EQUAL

Although Fourth Amendment jurisprudence highly favors protecting the sanctity of the home, the collection of real-time CSLI—just like the collection of

---

188. *Hammond*, 996 F.3d at 387 n.4 ("On appeal, the government clarifies that it did not concede that the Fourth Amendment applies to Hammond's real-time CSLI. To the contrary, in its response to Hammond's motion to suppress, the government 'accept[ed] for the sake of argument (without conceding) that real-time data is subject to the same Fourth Amendment protections as historical data.'").

189. *Id.* at 389.

190. *Id.*

191. *Id.* at 388 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).

192. *Id.* at 389 (citing *Carpenter*, 138 S. Ct. at 2218).

193. *Id.* at 390.

194. *Id.*

195. *Id.* (citing *Carpenter*, 138 S. Ct. at 2217).

196. *Id.* (citing *Carpenter*, 138 S. Ct. at 2217).

historical CSLI—has a dangerous ability to invade these private spheres.[197] Establishing a warrant requirement for real-time CSLI will ensure that private spheres continue to be highly protected by the Fourth Amendment and that law enforcement does not exceed the scope of reasonable surveillance as outlined in *Carpenter*.[198] Importantly, establishing a warrant requirement will still allow for exceptions (such as exigency) so as not to infringe on law enforcement's ability to deter criminal activity.

The mosaic approach adopted in *Hammond* is problematic for several reasons. First, it does not acknowledge that individuals maintain a reasonable expectation of privacy in their real-time CSLI and that they do not meaningfully waive this right by disclosing their location information to their cell phone company. Second, it fails to set limits on law enforcement's unfettered access to ever-changing technology, which exceeds traditional means of surveillance. Third, requiring a case-by-case analysis of extraneous factors provides no preemptive guidance for law enforcement and thus results in inconsistent protections for the public.

A. Individuals Maintain a Reasonable Expectation of Privacy in Their Real-time CSLI

When subjected to a *Katz* test, there is no meaningful difference between historical CSLI and real-time CSLI. The first prong of the test—subjective expectation of privacy—is satisfied because Americans do not consent to "warrantless government access" simply by choosing to carry a cell phone.[199] Nevertheless, the subjective prong of this test has been "minimized" by the Supreme Court over time, and the breadth of the analysis now lies in the second prong—whether society is prepared to deem the expectation of privacy as reasonable.[200] The second prong is also satisfied here because individuals maintain a right to privacy in their public movements and neither waive this privacy by choosing to carry a cell phone nor anticipate that law enforcement will have an unrestricted ability to force their cell phones into revealing their location at any moment wherever they are.

The mosaic courts maintain that individuals do not have a reasonable expectation of privacy in their movements as collected by real-time CSLI because real-time CSLI does not collect retrospective data.[201] But, although real-time CSLI is not collected retrospectively, it still has a comparable ability to create a

---

197. *See* Payton v. New York, 445 U.S. 573, 586 (1980) (recognizing "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.").

198. *Carpenter*, 138 S. Ct at 2218.

199. *See* Tracey v. State, 152 So. 3d 504, 523 (Fla. 2014) ("Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion . . . places an unreasonable burden on the user to forego necessary use of his cell phone.).

200. *See Carpenter*, 138 S. Ct at 2238 (Thomas, J., dissenting) (citing Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015)).

201. *See Hammond*, 996 F.3d at 390.

comprehensive record of an individual's movements and can similarly traverse into private spaces. This intrusion was illustrated in *Pacheco* where law enforcement consistently monitored the real-time CSLI of their suspect for 24 hours a day, 7 days a week, for 108 days.[202] Although the data collected in *Pacheco* was not collected retrospectively, it still had the capacity to implicate significant privacy concerns.[203] In fact, law enforcement tracking of the suspect in *Pacheco* had no limitations at all as to the "time of day or geographic location, including private residences,"[204] which exemplifies exactly the Court's qualms in *Carpenter*—that a cell phone faithfully follows its user into "private residences, doctor's offices, political headquarters, and other potentially revealing locales."[205] Officers would simply not have access to ninety-seven percent of Americans' locations without cell phones[206] and would not have the resources to perform such comprehensive investigations without the ease and efficiency of real-time CSLI collection.

Indeed, cell phone users cannot protect themselves from pings—or real-time CSLI monitoring—any more than they can protect themselves against historical CSLI monitoring.[207] Real-time CSLI is "catalogued through no action of the subscriber"[208] and cell phone users cannot circumvent this process without disconnecting the phone from its network entirely.[209] Although historical data is already being passively collected by cell phone companies, the collection of real-time CSLI is a process that is "initiated and effectively controlled" by law enforcement.[210]

Interestingly, although the Seventh Circuit held that society is not prepared to recognize a reasonable privacy interest in real-time CSLI, all three states that sit within its jurisdiction clearly *are* prepared to recognize such an expectation as reasonable—as evidenced by their legislation.[211] As discussed in further detail below, Indiana's law was passed following substantial public concern that Indiana State Police had purchased a stingray—allowing it to simultaneously track a large group of cell phone users in real-time while circumventing the cell phone company altogether.[212] The Illinois law was passed directly in response to

---

202. Commonwealth v. Pacheco, 263 A.3d 626, 649 (Pa. 2021).

203. *Id.* at 640-41.

204. *Id.* at 642.

205. *Carpenter*, 138 S. Ct at 2218.

206. *Mobile Fact Sheet, supra* note 4.

207. Laura Hecht-Felella, *The Fourth Amendment in the Digital Age,* BRENNAN CTR. FOR JUST. 14 (Mar. 18, 2021), https://www.brennancenter.org/sites/default/files/2021-03/Fourth-Amendment-Digital-Age-Carpenter.pdf [https://perma.cc/Z37A-49MU].

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

209. *See Carpenter*, 138 S. Ct. at 2220; *see also Sims*, 569 S.W.3d at 646 n.1.

210. Commonwealth v. Almonor, 120 N.E.3d 1183, 1193 (Mass. 2019).

211. *See* WIS. STAT. § 968.373(2) (2022); IND. CODE § 35-33-5-12(b) (2022); 725 ILL. COMP. STAT. ANN. 168/10 (West 2022).

212. *See* Ryan Sabalow, *Indiana State Police Tracking Cellphones – But Won't Say How or*

Carpenter, ensuring that the warrant requirement articulated in *Carpenter* for historical CSLI was also extended to real-time CSLI.[213] Wisconsin's law, which also requires a warrant supported by probable cause prior to tracking a cell phone's location, was signed into law in 2014 with bipartisan support and no opposition.[214]

B. Ever-growing Technology Requires Judicial Oversight to Avoid Privacy Intrusions

These states have taken issue with law enforcement's ability to exceed traditional means of surveillance, essentially attaching an "ankle monitor" on every cell phone user.[215] However, the mosaic courts do not address the loss of privacy to citizens in allowing law enforcement unfettered access to this sophisticated means of surveillance without judicial oversight. As illustrated by Justice Sotomayor in her *Jones* concurrence, "[a]wareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[216] Although some courts posit that "[b]ig government using powerful technology provided by large private companies to surreptitiously track the whereabouts of American citizens spells trouble for the basic constitutional rights of all"[217] others argue that it is poor practice to allow criminals—but not the police—to benefit from advancing technology.[218] In either case, without Congressional intervention, neither citizens nor law enforcement have a clear set of expectations. Presently, it seems that only those who avoid using a cell phone altogether can escape the omnipresent risk of being tracked in real-time.

C. Privacy Interests Should Not Be Limited by Length of Time or Location

The case-by-case approach adopted by the mosaic courts requires an analysis of whether the length of the real-time CSLI tracking constitutes a search and

---

Why, INDYSTAR (Dec. 9, 2013, 1:18 PM), https://www.indystar.com/story/news/2013/12/08/indiana-state-police-tracking-cellphones-but-wont-say-how-or-why/3908333/ [https://perma.cc/YTL3-VWXK].

213. *See HB 2134: Carpenter Location Tracking Fix,* ACLU ILL. (Aug. 23, 2019), https://www.aclu-il.org/en/legislation/hb-2134-carpenter-location-tracking-fix [https://perma.cc/JD5C-RNBG].

214. *What Police Must Now Have If They Want To Track a Cell Phone.* FOX6 MILWAUKEE (Apr. 23, 2014), https://www.fox6now.com/news/what-police-must-now-have-if-they-want-to-track-a-cell-phone [https://perma.cc/H6VB-DKZD].

215. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

216. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

217. United States v. Griggs, No. 2:20-CR-20403-1, 2021 WL 3087985, at *5 (E.D. Mich. July 22, 2021).

218. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012), *cert. denied,* 570 U.S. 919 (2013) ("The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools," otherwise "technology would help criminals but not the police.").

whether the real-time CSLI tracking was conducted while the individual was in a constitutionally protected area.[219] The length of time consideration presents a significant line-drawing problem. It requires an after-the-fact analysis of whether a particular search exceeded an ambiguous length of monitoring such that it entered Fourth Amendment search territory. Although real-time CSLI might be collected only long enough to apprehend a suspect, even a few hours of tracking can reveal intimate details of an individual's life.

Even if real-time CSLI tracking does not extend long enough to trigger constitutional protections, courts are further required to determine whether the tracked individual was present in a constitutionally protected area at the time of the search. There is, of course, no way for law enforcement to know whether the tracked individual is in a public space or in a constitutionally protected area until after the intrusion into their privacy has already occurred. Although Supreme Court precedent has identified a diminished expectation of privacy on public roads, the pertinent question is *how* officers came to find the individual.[220] For instance, in *Hammond*, law enforcement relied exclusively on the collection of real-time CSLI to locate their suspect.[221]

Although the *Carpenter* holding specified that an individual does not waive *all* Fourth Amendment rights venturing onto public roads,[222] *Hammond* stipulated that individuals expect "law enforcement's prying eyes" to be watching while they are in the public sphere.[223] Certainly, drivers (particularly those who receive speeding tickets) are accustomed to encountering officers on their morning commute, but they are not accustomed to law enforcement's ability to conduct remote surveillance from the comfort of their desks. In fact, the traditional type of visual, on-the-ground, surveillance described in *Hammond* has practical limitations that are not present with remote pinging and tracking. Although traditional surveillance is time-consuming and costly, real-time CSLI tracking is easy and cheap.[224]

Moreover, traditional surveillance cannot invade a constitutionally protected area without a warrant supported by probable cause.[225] The Fourth Amendment has "drawn a firm line at the entrance to the house," but officers conducting remote surveillance have no idea if they have crossed this firm line until after the intrusion has already occurred.[226] Although the *Hammond* decision highlighted the fact that there were no intimate details revealed by the officer's real-time search, this lucky coincidence does not justify a real-time search of individuals

---

219. *See* United States v. Hammond, 996 F.3d 374, 389 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022).

220. United States v. Knotts, 460 U.S. 276, 281 (1983).

221. *Hammond*, 996 F.3d at 381; *see supra* Part IV.

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

223. *Hammond*, 996 F.3d at 390.

224. *See Carpenter,* 138 S. Ct. at 2217-18.

225. *See* Payton v. New York, 445 U.S. 573, 586-87 (1980).

226. *Id.* at 590.

at any time.[227] Even prior to *Carpenter*, courts took issue with the post hoc nature of the analysis employed by the Seventh Circuit in *Hammond*.[228] Although the officers in *Hammond happened* to track Hammond's location at a time when he *happened* to be on public roads, there is no way of knowing where a suspect will be until after the "incursion into a citizen's private affairs has already taken place."[229]

Because of the similarities between historical CSLI and real-time CSLI, there is little justification for treating these two types of location information differently. The collection of both types of data necessitates law enforcement's infringement into records kept by cell phone companies, and cell phones have become such a pervasive part of our lives that opting not to carry them is simply not feasible. Real-time CSLI, just like historical CSLI, allows law enforcement to create a comprehensive dossier of an individual's movements. Real-time CSLI presents even greater privacy concerns than historical CSLI because it is collected at the behest of law enforcement through pings. Further, both types of data take advantage of ever-growing technology, and allowing law enforcement access to such technology without judicial oversight predisposes it to abuse.

D. State Legislative Efforts

State legislative efforts were sparked in response to concerns that advancing location technology would violate cell phone users constitutional right to privacy if proper checks and balances were not implemented.[230] Illustrative is a controversy in Indiana wherein Indiana State Police ("ISP") purchased a Stingray and refused to confirm that they possessed it.[231] In response, legislators passed Indiana Code Section 35-33-5-12.[232] The Stingray allowed law enforcement to collect real-time CSLI (and other information such as text messages and call logs) from a large group of people simultaneously without having to go through a cell phone company to track a specific suspect.[233] Following a data leak from the National Security Agency ("NSA") by Edward Snowden and an investigation by the *Indianapolis Star*, ISP acknowledged that they had in fact purchased a

---

227. *Hammond*, 996 F.3d at 389.

228. *See, e.g.,* Commonwealth v. Pitt, No. 2010-0061, 2012 WL 927095, at *7 (Mass. Super. 2012) ("[T]he Fourth Amendment's warrant requirement cannot protect citizens' privacy if a court determines whether a warrant is required only after the search has occurred . . . ."); s*ee also* Tracey v. State, 152 So. 3d 504, 521 (Fla. 2014) ("Ad hoc, after-the-fact determination of whether real time [CSLI] monitoring constitute[s] a Fourth Amendment violation presents [the] . . . danger of arbitrary and inequitable enforcement.").

229. *See Pitt*, 2012 WL 927095, at *7.

230. Sabalow, *supra* note 212.

231. *Id.*

232. *See* Barb Berggoetz, *Legislature on Verge of Restricting Digital Surveillance*, INDYSTAR (Feb. 7, 2014, 6:25 PM), https://www.indystar.com/story/news/2014/02/07/legislature-on-verge-of-restricting-digital-surveillance/5293463/ [https://perma.cc/QP99-35C8].

233. *Id.*

Stingray but refused to disclose what "due process" determined their use of it (even to an Indiana State Senator).[234]

In response to concerns over the NSA's "warrantless cellphone spying"[235] and ISP's ability of to track cell phones without "judicial and legislative oversight,"[236] the Indiana Code mandated that "a law enforcement officer . . . may not use a real time tracking instrument . . . unless . . . [they have] *obtained an order issued by a court based upon a finding of probable cause*."[237] The code offers an exigency exception but requires officers who use this exception to seek an order by the court "not later than seventy-two (72) hours after the initial use of the real time tracking instrument."[238] At least twelve other states have enacted similar legislation requiring a warrant supported by probable cause, including California,[239] Colorado,[240] Illinois,[241] Maine,[242] Maryland,[243] Minnesota,[244]

---

234. Senator D. Brent Waltz, *Privacy in the Digital Age*, 48 IND. L. REV. 205, 210 (2014) ("[ISP] stated that [it] would 'consult' with a judge before the device was deployed but refused to share what, if any, restraints they felt obliged to abide by."); *see* Sabalow, *supra* note 212 ("[T]hey won't even say whether they ask a judge for a search warrant . . . .").

235. Berggoetz, *supra* note 232.

236. Waltz, *supra* note 234, at 210.

237. IND. CODE § 35-33-5-12(a)(1) (2022) (emphasis added). The Indiana Code does not define "real time tracking instrument," but legislators acknowledged that because advancing technology evolves faster than the law, the bill is intended to provide a framework upon which future privacy concerns can be considered, to provide law enforcement with guidelines, and to give Hoosiers the peace of mind that their "reasonable expectations of privacy are still guaranteed." *Rep. Koch's Privacy Bill Signed into* Law, IND. HOUSE OF REPRESENTATIVES REPUBLICAN CAUCUS (Apr. 22, 2014, 7:00 PM), https://www.indianahouserepublicans.com/news/press-releases/r65-rep.-koch-s-privacy-bill-signed-into-law-4-22-2014/ [https://perma.cc/X8Q4-YEPM]).

238. IND. CODE § 35-33-5-12(b) (2022).

239. CAL. PENAL CODE § 1546.1(b)(1) (West 2022) ("A government entity may compel the production of or access to electronic communication information . . . only . . . pursuant to a warrant . . . .").

240. COLO. REV. STAT. § 16-3-303.5(2) (2022) ("[A] government entity shall not obtain the location information of an electronic device without a search warrant issued by a court.").

241. 725 ILL. COMP. STAT. ANN. 168/10 (2019) ("[A] law enforcement agency shall not obtain location information . . . without first obtaining a court order . . . based on probable cause.").

242. ME. STAT. tit. 16, § 648 (2022) ("[A] government entity may not obtain location information without a valid warrant.").

243. MD. CODE ANN., CRIM. PROC. § 1-203.1(b)(1) (West 2022) ("A court may issue an order authorizing or directing a law enforcement officer to . . . obtain location information from an electronic device after determining . . . that there is probable cause . . . .").

244. MINN. STAT. § 626A.42(2) (2022) ("[A] government entity may not obtain the location information . . . without a tracking warrant. A warrant granting access to location information must be issued only if the government entity shows that there is probable cause . . . .").

Montana, [245] New Hampshire,[246] Tennessee,[247] Utah,[248] and Wisconsin.[249]

Despite state legislation requiring that law enforcement obtain a warrant supported by probable cause prior to obtaining real-time CSLI, the mosaic courts add their own nuances to the issue. Moreover, federal courts may view state legislation as irrelevant.[250] Even when state law requires a warrant for real-time CSLI tracking, state law is not honored if the target of the search ends up in federal court because "[v]iolations of state law do not justify suppression in federal prosecutions."[251] If consistency and predictability are the goals, then a congressional act is the proper course of action.

E. Previous Federal Attempts and a Call to Action

Bipartisan federal efforts have previously been made[252] to implement a probable cause warrant requirement for the collection of location information, and these efforts largely equated real-time and historical data.[253] In an attempt to "balance the needs of the police with the expectations of privacy of those that

---

245. MONT. CODE ANN. § 46-5-110(1)(a) (2022) ("[A] government entity may not obtain the location information of an electronic device without a search warrant.").

246. N.H. REV. STAT. ANN. § 644-A:2(I) (2022) ("[A] government entity shall not obtain location information from an electronic device without a warrant issued by a judge based on probable cause.").

247. TENN. CODE ANN. § 39-13-610(b) (2022) ("[N]o governmental entity shall obtain the location information of an electronic device without a search warrant issued by a duly authorized court.").

248. UTAH CODE ANN. § 77-23c-102(1)(a)(i) (West 2022) ("[A] law enforcement agency may not obtain, without a search warrant issued by a court upon probable cause: . . . the location information.").

249. WIS. STAT. § 968.373(2) (2022) ("[N]o investigative or law enforcement officer may identify or track the location of a communication device without first obtaining a warrant.").

250. *See, e.g.*, United States v. Hammond, No. 3:18-CR-5 RLM-MGG, 2018 WL 5292223 at *4.

251. *Id.* (quoting United States v. Castetter, 865 F.3d 977, 978-79 (7th Cir. 2016), *cert. denied*, 138 S. Ct. 1281 (2018)).

252. *See, e.g.*, *Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the Comm. on the Judiciary,* 112th Cong. (2012) [hereinafter 2012 Hearing]. The GPS Act was reintroduced in the 113th and 114th Congresses—but each time it failed to move forward. *Geolocation Privacy Legislation,* GPS.GOV, https://www.gps.gov/policy/legislation/gps-act/ [https://perma.cc/PY5V-324D] (last visited Nov. 21, 2021). And in 2017, the bill was again reintroduced—the legislation was referred to the Committee on the Judiciary and the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations—but saw no further action. *Actions: H.R.3470 - GPS Act,* CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/house-bill/3470/all-actions?s=1&r=36 [https://perma.cc/ QW2N-ZQMD] (last visited Nov. 21, 2021).

253. *See* Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013).

they protect,"[254] Representative Jason Chaffetz introduced the Geolocation Privacy and Surveillance (GPS) Act in 2012.[255] This bill sought to "create[] a legal framework . . . to give government agencies, commercial entities and private citizens clear guidelines for when and how geolocation information can be accessed and used."[256] Specifically, the bill would require a probable cause warrant from a judge to track a person's location.[257] Notably, the bill did not distinguish between historical and real-time tracking, instead requiring a warrant supported by probable cause for both.[258]

Interestingly, opponents of the bill specifically took issue with the probable cause requirement for historical CSLI.[259] In 2012, prior to the *Carpenter* holding, opponents to the probable cause requirement encouraged legislators to differentiate between historical data and real-time data.[260] Opponents wanted to preserve a lower legal standard for the collection of historical CSLI because the "overwhelming majority [of] request[s]" by law enforcement were for historical data, and law enforcement widely used historical data to confirm whether a suspect was present at the location where a crime previously took place.[261]

This opposition to a probable cause requirement continued at the 2016 hearing, where opponents again requested a distinction between historical and real-time CSLI and explicitly stated they opposed a probable cause warrant requirement *only* for historical tracking.[262] In fact, a representative from the Department of Justice ("DOJ") specified that the DOJ agrees a warrant is required for real-time tracking,[263] reasoning that people are more entitled to an expectation of privacy in their real time movements than in their historical movements.[264] Legislators disagreed that there was any viable distinction between historical and real-time CSLI, specifying that they found the distinction between the two

---

254. 2012 Hearing, *supra* note 252, at 2 (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec.).

255. *Id.* at 1, 22.

256. *Id.* at 22 (statement of Rep. Jason Chaffetz, Member, Subcomm. on Crime, Terrorism, and Homeland Sec.).

257. *Id.* at 23.

258. *See* Online Communications and Geolocation Protection Act Geolocational Privacy and Surveillance Act, H.R. 983, 113th Cong. § 3 (2013).

259. 2012 Hearing, *supra* note 252, at 27.

260. *Id.*

261. *Id.* (testimony of Joseph I. Cassilly, Past President, Nat'l Dist. Att'ys Ass'n).

262. *2016 Hearing*, *supra* note 6, at 72.

263. *Id.* (statement of Richard Downing, Deputy Chief, Comput. Crime & Intell. Prop. Section U.S. Dep't of Just.). "We have taken the position publicly that we do not need . . . a warrant for historic cell location information. If we were to use real-time tracking . . . we, yes, agree a warrant is required in that circumstance." *Id.*

264. *Id.* at 73 ("[W]hether somebody is being tracked in real time going forward has historically been recognized as something that is more intrusive than looking at a historical view of somebody's activities.").

altogether "stupid and meaningless."[265]

Because the Supreme Court has since held that a warrant supported by probable cause is required for historical CSLI,[266] and because there seemed to be little disagreement that real-time CSLI should require a warrant supported by probable cause, it is high time for Congress to revisit a version of the bill that grants equal protection for both types of data. Because both the proponents and opponents of the bill agreed that real-time CSLI presents sufficient privacy concerns to justify a probable cause warrant requirement, a new version of the bill will likely be met with less controversy.

Further, it is possible that anything short of a probable cause warrant requirement might be overturned by the Supreme Court.[267] The Stored Communications Act ("SCA"), passed by Congress in 1986, required only "*reasonable grounds* to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[268] Prior to the *Carpenter* decision, law enforcement relied on this lesser standard to gain access to an individual's CSLI with a mere showing of reasonable grounds.[269] However, in *Carpenter*, the Supreme Court specified that "an order issued under [the SCA] is not a permissible mechanism for accessing historical [CSLI]" instead requiring that the Government "get a warrant" prior to such a search.[270]

CONCLUSION

In *Hammond*, the Seventh Circuit held that the short-term collection of real-time CSLI did not constitute a Fourth Amendment search where it did not traverse into a constitutionally protected area.[271] However, law enforcement's warrantless collection of real-time CSLI presents many of the same privacy concerns that troubled the Supreme Court in *Carpenter*.[272] Individuals maintain an expectation of privacy in their location as tracked by real-time CSLI and do not waive this right to privacy by virtue of owning and using a cell phone throughout the day, particularly when cell phones have virtually become a requirement of existing in the modern world. The nuanced examination adopted by the Seventh Circuit was not envisioned by state legislation and requires an inefficient, after-the-fact analysis which does little to protect Fourth Amendment privacy rights. Requiring a warrant supported by probable cause will ensure

---

265. *Id.* (statement of Rep. Ted Lieu, Member, Comm. on Oversight and Gov't Reform).

266. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

267. *See id.* (holding that collection of historical CSLI was a search even though an order was issued by a magistrate judge pursuant to the SCA); *see also* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J.F. 943, 944 (2019).

268. 18 U.S.C. § 2703(d) (emphasis added).

269. *See id.*

270. *Carpenter*, 138 S. Ct. at 2221.

271. United States v. Hammond, 996 F.3d 374, 392 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 2646 (2022).

272. *Carpenter*, 138 S. Ct. at 2221.

adequate constitutional protection, while also allowing for exceptions when needed—such as in an exigent circumstance.

Prior attempts for a federally mandated probable cause warrant requirement have failed largely due to contention with a probable cause requirement for historical CSLI.[273] Now that the Supreme Court identified a reasonable expectation of privacy in historical CSLI, it is "ripe for Congress to make clear"[274] that both historical and real-time CSLI are entitled to legislative protection or for the Supreme Court to clarify the proper analysis.

273. *See* discussion *supra* Section V.E.

274. *2016 Hearing*, *supra* note 6, at 76 (statement of Neema Singh Guliani, Legislative Counsel, ACLU).