Privacy After *Carpenter v. United States*: Can a Tower Dump Warrant Meet the Warrant Requirement?

Sarah Bramley-Garoutte*

"[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."[1]

I. INTRODUCTION

Cell phone users create a detailed, time-stamped record of their movements everywhere they carry their phone.[2] Cell site location information (CSLI) refers to this record that cell phones send to the user's service provider (provider).[3] Beyond turning the cell phone off or disconnecting it from the cellular network, there is no way for users to avoid creating CSLI.[4] Consequently, the vast majority of adults in America are sending mass amounts of location data to their providers.[5] Providers store CSLI along with personal identifiable information (PII)

* J.D. Candidate, Suffolk University Law School, 2023; B.S. Southern Oregon University, 2019. I would first like to thank Professor René Reyes, whose expertise and thoughtful guidance was vital in the creation of this Note. I would also like to thank all *Suffolk University Law Review* editors and staff members for their tireless work and thoughtful contributions. Lastly, special thanks to my family and friends for their unconditional love and support.

1. Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

2. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) (explaining location information generated every time cell phones connect to cell sites); Mason Kortz & Christopher Bavitz, *Legal Analysis: Cell Tower Dumps*, 63 BOS. BAR J. 27, 27 (2019) (describing how networks track users at any given time).

3. *See Carpenter*, 138 S. Ct. at 2211 (defining CSLI); Kortz & Bavitz, *supra* note 2, at 27 (providing technical overview of CSLI creation and transmission); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner at 3, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (noting cell phones' automatic generation of location data); RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUST., CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY 1 (2018), https://www.brennancenter.org/media/125/download [perma.cc/LGU2-2SGY] (detailing CSLI generation and collection); Deepali Lal, Comment, *Technology in the Modern Era: The Implications of* Carpenter v. United States *and the Limits of the Third-Party Doctrine as to Cell Phone Data Gathered Through Real-Time Tracking, Stingrays, and Cell Tower Dumps*, 43 U. ARK. LITTLE ROCK L. REV. 519, 519 (2021) (asserting CSLI continuously gathered from every cell phone).

4. *See Carpenter*, 138 S. Ct. at 2211 (acknowledging cell phones generate CSLI even when phone features not used); LEVINSON-WALDMAN, *supra* note 3, at 2 (explaining near impossibility of stopping CSLI transmission while cell phone on).

5. *See Carpenter*, 138 S. Ct. at 2211-12 (noting modern cell phones generate vast amounts of CSLI); *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/7SK2-JLPF] (claiming majority of adults own smart phones).

about cell phone users.[6] Yet providers are not the only ones with access to this information—providers often grant access of CSLI and PII to law enforcement for criminal investigations.[7] Government officials, including law enforcement and prosecutors, can even request the CSLI and PII of all users who connected to cell sites in a certain area during a specified time—including those who have not even been suspected of a crime—which is termed a cell tower dump.[8]

Technological advances like CSLI have implicated the general public's privacy concerns, but the Supreme Court has continually iterated its support for preserving the degree of privacy that existed at the time of the Fourth Amendment's adoption.[9] This support has not been without great exception, however, as the Court previously established in the third-party doctrine that one does not have a legitimate expectation of privacy in information they voluntarily share with third parties.[10] In *Carpenter v. United States*, the Supreme Court readdressed the third-party doctrine in answering whether the Fourth Amendment protects historical CSLI—seven days or more of a user's CSLI.[11] In this

6. *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 15 (2013) (explaining providers store vast amounts of subscriber information law enforcement may later request).

7. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2212 (detailing law enforcement's request of Carpenter's historical CSLI); United States v. James (*James II*), 3 F.4th 1102, 1104 (8th Cir. 2021) (explaining how law enforcement identified defendant through tower dump request); United States v. Hammond, 996 F.3d 374, 381 (7th Cir. 2021) (outlining law enforcement's process of identifying defendant through real-time and historical CSLI).

8. *See* Owsley, *supra* note 6, at 18 (noting large numbers of users potentially caught in cell tower dumps); LEVINSON-WALDMAN, *supra* note 3, at 2 (explaining differences between types of location data); Emma Lux, Article, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. ONLINE 109, 109-10 (2020) (discussing broad reach of tower dumps affecting innocent users).

9. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (outlining Fourth Amendment protections and technological advances); Kyllo v. United States, 533 U.S. 27, 34 (2001) (confronting limits of technology to assure privacy preserved); United States v. Jones, 565 U.S. 400, 402 (2012) (addressing question of whether GPS tracking implicates Fourth Amendment); Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding wiretap not search under Fourth Amendment), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); *see also* Lux, *supra* note 8, at 110 (noting tower dumps implicate mass amounts of data). In support of preserving this degree of privacy, the Court has pointed to some of its previous decisions: In *Kyllo*, it held unconstitutional the use of thermal imaging technology to gain otherwise unknowable details about the inside of the home, and in *Riley v. California*, it required law enforcement to secure a warrant before searching a cell phone because of the vast collection of personal data. *See Carpenter*, 138 S. Ct. at 2214 (detailing previous decisions); *see also Kyllo*, 533 U.S. at 35 (rejecting government's interpretation of Fourth Amendment); Riley v. California, 573 U.S. 373, 403 (2014) (noting cell phones contain "the privacies of life" for many Americans).

10. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding no legitimate expectation of privacy in telephone numbers dialed); United States v. Miller, 425 U.S. 435, 443 (1976) (ruling Fourth Amendment does not protect bank records because of voluntary disclosure to third party).

11. *See Carpenter*, 138 S. Ct. at 2217, 2221 (declining to extend *Miller* because of CSLI's depth and breadth of information captured). The Court has repeatedly held the government does not need a warrant to obtain an individual's information voluntarily conveyed to a third party. *See, e.g.*, *Miller*, 425 U.S. at 443 (determining bank records contained voluntarily conveyed information and not subject to Fourth Amendment warrant requirement); *Smith*, 442 U.S. at 743-44 (holding telephone numbers dialed do not implicate Fourth Amendment warrant requirement); United States v. Knotts, 460 U.S. 276, 281-82 (1983) (applying third-party doctrine to use of beeper in tracking suspect). In *Carpenter*, however, the Court determined that the fact the cell phone user provided CSLI to a third party does not overcome the user's Fourth Amendment protections and concluded the government

landmark decision, the Court declined to extend the third-party doctrine to CSLI because of CSLI's unique nature.[12] The Court noted CSLI is inescapable tracking that follows every cell phone user.[13]

The Court's narrow holding in *Carpenter* clarified the protection afforded to historical CSLI but left tower dump and real-time CSLI unprotected.[14] As such, *Carpenter* has left lower courts to grapple with the distinction between tower dump CSLI, which can implicate thousands of user's location information, and the historical CSLI of one user; particularly, whether their differences warrant different treatment under the Fourth Amendment.[15] Perhaps due to the ongoing uncertainty, some states have enacted legislation requiring law enforcement to obtain a warrant for any CSLI—effectively prohibiting the government from conducting a warrantless tower dump.[16]

This Note examines the tension between the warrant requirements and a typical tower dump warrant that names no person or suspected phone number.[17] After detailing Fourth Amendment jurisprudence, Part II outlines CSLI jurisprudence.[18] Part III then compares a tower dump warrant to an "all-person" warrant prohibited under the Fourth Amendment while analyzing the warrant requirements.[19] This Note concludes by proposing how courts should limit law enforcement's use of tower dumps to comply with constitutional warrant requirements.[20]

---

needs a warrant for historical CSLI. *See Carpenter*, 138 S. Ct. at 2217, 2221. Prior to *Carpenter*, Justice Sotomayor suggested the third-party doctrine was ill-suited for the digital age and stated she would not assume that the Fourth Amendment does not protect information voluntarily disclosed to a third party for a limited purpose. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (reconsidering third-party doctrine in digital age).

12. *See Carpenter*, 138 S. Ct. at 2217 (holding one maintains reasonable expectation of privacy in movements). In so holding, the Court focused on the deeply revealing nature of CSLI and the inescapable, automatic collection by providers. *See id.* at 2223 (noting CSLI's depth, breadth, and comprehensive reach).

13. *See id.* at 2218 (discussing qualitative distinctions of CSLI).

14. *See id.* at 2267 (Gorsuch, J., dissenting) (questioning distinction between tower dump and historical CSLI); *see also In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 738 (N.D. Ill. 2020) (suggesting no reason for concluding seven days constitutes search).

15. *See* United States v. Walker, No. 18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *20-22 (E.D.N.C. July 20, 2020) (detailing differences between CSLI types); United States v. Adkinson, 916 F.3d 605, 611 (7th Cir. 2019) (indicating potential Fourth Amendment issue with tower dump CSLI); United States v. James (*James I*), No. 18-cr-216 (SRN/HB), 2018 U.S. Dist. LEXIS 210433, at *10-11 (D. Minn. Nov. 26, 2018) (declining to address reasonable expectation of privacy issue *Carpenter* left open).

16. *See* COLO. REV. STAT. § 16-3-303.5 (2023); 725 ILL. COMP. STAT. ANN. 168/10 (West 2022); ME. REV. STAT. ANN. tit. 16, § 648 (West 2022); MINN. STAT. ANN. § 626A.42 (West 2023); MONT. CODE ANN. § 46-5-110 (West 2022); N.H. REV. STAT. ANN. § 644-A:2 (2022); 12 R.I. GEN. LAWS § 12-32-2 (2022); TENN. CODE ANN. § 39-13-610 (2022); UTAH CODE ANN. § 77-23C-102 (LexisNexis 2022); VT. STAT. ANN. tit. 13, § 8102 (2022) (declaring warrant required for protected user information, including location information).

17. *See infra* Part III (highlighting tension between warrant requirements and tower dump warrants).

18. *See infra* Sections II.C, II.E (providing overview of Fourth Amendment jurisprudence and CSLI state legislation).

19. *See infra* Section III.B (analyzing whether tower dump warrants comply with warrant requirements).

20. *See infra* Section III.C (suggesting limitation of tower dumps to serial crime investigations).

II. HISTORY

A. CSLI

For cell phones to serve their intended purpose of providing a communication medium, they must send and receive data by wirelessly connecting to a cellular network through cell sites—antennas affixed to the company's cell towers or other tall structures.[21] Each cell tower generally has numerous cell sites facing different directions, and each cell site contains multiple antennas that allow cell phones to connect to the network.[22] As a user moves away from one cell tower and closer to another, their cell phone automatically transfers its connection to the strongest cell site.[23] Cell phones connect to cell sites both periodically while the cell phone is on and whenever the user initiates a function requiring a cellular connection.[24] While not every function on a cell phone requires a cellular connection, a cell phone must be able to connect to the network to send a text, make a call, use an application, or complete any other function which requires cellular connection.[25] Consequently, cell site connections may occur every few minutes, but can be as frequent as every seven seconds.[26]

---

21. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) (explaining how cell phones connect to network); Owsley, *supra* note 6, at 4 (clarifying cell sites found on both cell towers and other structures); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 2 (noting cell phones must connect to network for users to truly use).

22. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 6-7 (outlining how cell site antennas detect radio signals from cell phones for network connection). A provider's many cell towers and cell sites make up the company's cellular network. *See* Zachary R. Hoover, Article, *The Pervasion of Cell Phones and the Fourth Amendment: A Right to Privacy in Locational Data*, 46 CAP. U. L. REV. 739, 742 (2018) (detailing components of provider's network); Kortz & Bavitz, *supra* note 2, at 27 (stating cellular network composed of various cell sites and towers); Lal, *supra* note 3, at 535 (describing makeup of providers' cellular network).

23. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 7 (noting cell phones constantly look for strongest cell site for connection).

24. *See* Hoover, *supra* note 22, at 743 (explaining cell phones connect to cell sites actively and passively); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 7. A cell phone can tap into the network passively through functions the user does *not* initiate, including through apps continually running in the background. *See* Hoover, *supra* note 22, at 743 (highlighting cell phones generate location data for each active and passive connection); *see also* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 11 (arguing cell phones generate CSLI without user interaction partly because apps run in background). It is these continued passive connections that generate the bulk of CSLI. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 21.

25. *See* Hoover, *supra* note 22, at 743 (explaining active and passive cellular network connections); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 2 (stating cell tower connection essential for cell phone use).

26. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 11 (highlighting potential frequency of cell phone connection to cell towers); *see also* Hoover, *supra* note 22, at 746 (detailing cell phones connect passively every seven seconds); Owsley, *supra* note 6, at 5 (asserting cell phones connect to cellular network approximately every seven seconds).

For every cell site connection, cell phones generate and send location information to the user's provider that the provider then stores.[27] Providers typically retain CSLI for at least a year, but some large providers retain it indefinitely.[28] CSLI usually includes the date of the connection, start and end time of the connection, and the location of the connection.[29] Additionally, CSLI includes the user's phone number or unique identifier number so providers can identify which user connected to the network through that cell site.[30] Providers further maintain extensive records of PII, including an individual's name, address, call records, date of birth, social security number, driver's license number, and banking information.[31]

CSLI shows a cell phone's location and movements, both in the past and in real time.[32] Historical CSLI refers to the record of a user's past location data that law enforcement can request after the fact.[33] Real-time CSLI refers to location data of a user's movements as they occur.[34] Law enforcement can obtain real-time CSLI by requesting the provider "ping" the cell phone, which forces the cell phone to reveal its current location by connecting to the nearest cell site.[35]

The accuracy of CSLI depends upon the number of cell sites near the cell phone.[36] More cell sites mean smaller coverage areas, leading to cell phones

27. *See* Owsley, *supra* note 6, at 5 (noting cell site connection transmits information to provider); LEVINSON-WALDMAN, *supra* note 3, at 1-2 (summarizing cell phone location data collection); Hoover, *supra* note 22, at 743 (explaining cell phones transmit location data to providers who store it).

28. *See* Owsley, *supra* note 6, at 21 (discussing storage length of CSLI by cell providers); *Cell Phone Location Tracking Public Records Request*, ACLU (Mar. 25, 2013), https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request?redirect=locationtracking [https://perma.cc/D6C7-VJ5C] (suggesting providers may store CSLI indefinitely). Providers collect and retain CSLI for various business purposes, including for finding weak spots in the network and applying roaming charges. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (noting providers also sell location records to data brokers). While providers have long collected CSLI from incoming calls, they now also collect CSLI from text messages and other typical data connections. *See id.* (explaining providers' business purposes behind collecting CSLI).

29. *See* Hoover, *supra* note 22, at 743 (listing information included in CSLI providers typically collect).

30. *See* Owsley, *supra* note 6, at 15 (listing subscriber information stored by cell phone providers and requested by law enforcement officials).

31. *See id.*; United States v. Walker, No. 2:18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *5-9 (E.D.N.C. July 20, 2020) (outlining detailed user information law enforcement requested from providers); United States v. Rhodes, No. 19-CR-0073-AT-LTW, 2020 U.S. Dist. LEXIS 253307, at *3 (N.D. Ga. June 16, 2020) (noting law enforcement requested personal identifiers from providers).

32. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (discussing historical CSLI and real-time CSLI).

33. *See Carpenter*, 138 S. Ct. at 2212 (describing historical records of Carpenter's CSLI obtained); Kortz & Bavitz, *supra* note 2, at 27 (explaining historical CSLI refers to one user's CSLI).

34. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (defining prospective CSLI).

35. *See id.* (noting various ways law enforcement can request real-time location information); Commonwealth v. Almonor, 120 N.E.3d 1183, 1187 (Mass. 2019) (discussing how law enforcement had phone company force suspect's phone to reveal real-time location). A "ping" compels the cell phone to emit a signal that then transmits the user's real-time location information to the provider. *See Almonor*, 120 N.E.3d at 1193.

36. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211-12 (2018) (explaining increased installation of cell sites, particularly in urban areas); Hoover, *supra* note 22, at 744 (discussing how accuracy of CSLI varies depending on cell site density); Owsley, *supra* note 6, at 4 (suggesting cell site numbers depend in part on density of cell phone users); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 2 (noting more cell sites equates to greater location precision).

transmitting more precise location data to providers.[37] While varying cell site numbers means the accuracy of a user's location will depend on the area traveled, CSLI can usually show the user's location down to a few hundred feet or less.[38] As technology has advanced, the precision of CSLI has increased and has approached that of GPS.[39] Providers are also installing more cell sites to handle the growing data usage by more users, leading to ever smaller coverage areas.[40] Some cell sites even employ newer, more advanced technology that allows CSLI to place a user down to the floor of a building.[41]

B. Tower Dump

When law enforcement submits a tower dump request, providers generate a report of CSLI for all users that connected to a cell site within the specified location and time range.[42] This report generally includes the user's cell phone number and CSLI—a record of the date, start and end time, the location, and tower side of the cell site connection.[43] Additionally, because providers collect extensive amounts of PII, law enforcement can request providers also disclose the desired PII of ensnared users.[44] Although providers are required by law to maintain and protect CSLI and PII, they receive frequent requests for this data from law enforcement and will disclose it if law enforcement has complied with

37. *See supra* note 36.

38. *See Carpenter*, 138 S. Ct. at 2211-12 (noting increasing cell site coverage in urban areas); Hoover, *supra* note 22, at 745 (providing overview of CSLI accuracy); Kortz & Bavitz, *supra* note 2, at 27 (outlining range of accuracy).

39. *See* Hoover, *supra* note 22, at 745; Owsley, *supra* note 6, at 6 (summarizing new technology behind CSLI's improving accuracy). Over ten years ago, top law enforcement officials suggested CSLI was accurate enough to show if a user was in their home, and accuracy has only increased since then. *See* Hoover, *supra* note 22, at 744 (providing testimony from FBI agent regarding CSLI accuracy).

40. *See supra* note 36.

41. *See* Commonwealth v. Perry (*Perry II*), 184 N.E.3d 745, 753 (Mass. 2022) (explaining "small cell" technology and its increasingly ubiquitous nature). Providers utilize smaller cell sites—known as "microcells," "picocells," or "femtocells," inside of buildings to expand coverage. *See* Owsley, *supra* note 6, at 4 (discussing provider's uses of cell sites in its coverage); *Perry II*, 184 N.E.3d at 753 (noting some areas utilize "small cell" technology, resulting in greater precision).

42. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (explaining nature of tower dump); Kortz & Bavitz, *supra* note 2, at 27 (comparing tower dump CSLI and historical CSLI); LEVINSON-WALDMAN, *supra* note 3, at 2 (detailing various ways law enforcement utilizes CSLI in tracking user locations); Owsley, *supra* note 6, at 2. By its nature, a tower dump involves access to a greater number of users' CSLI than historical CSLI because it involves the data of every user whose cell phone connected to specific cell sites during a set interval. *See* Kortz & Bavitz, *supra* note 2, at 27; Lux, *supra* note 8, at 109-10 (distinguishing historical CSLI from tower dump CSLI). Arguably, the level of intrusion in a tower dump is less than that of historical CSLI because tower dumps usually cover a limited area over a short time period. *See* Kortz & Bavitz, *supra* note 2, at 28 (suggesting tower dumps reveal less about users' movement than historical CSLI); Lux, *supra* note 8, at 110 (acknowledging tower dump likely yields less CSLI about one specific user than historical CSLI).

43. *See* Hoover, *supra* note 22, at 743.

44. *See* Owsley, *supra* note 6, at 15 (outlining available information including name, address, social security number, call records, service records, and more).

applicable law and policy.[45] While courts disagree as to whether PII is disclosed alongside CSLI in a tower dump report, law enforcement may choose to originally request disclosure of both, and providers will usually comply.[46] As noted by the Supreme Court, the gathering of CSLI from providers is cheap, easy, and efficient when compared to traditional investigative techniques.[47]

Under the Stored Communications Act (SCA), law enforcement has warrantlessly requested CSLI from providers for over a decade.[48] Providers have faced an increasing number of requests for CSLI in recent years, including for tower dumps.[49] As providers retain CSLI records, law enforcement is able to request a cell phone user's recent and historical movements, spanning back years.[50] A

45. *See* Stored Communications Act, 18 U.S.C § 2703(d); Owsley, *supra* note 6, at 15, 17 (suggesting law enforcement routinely requests PII along with CSLI from providers). Some providers even give law enforcement manuals on how to request CSLI and PII to comply with the provider's own policies. *See* Hoover, *supra* note 22, at 748 (stating providers often provide manuals with procedures to collect desired information); Owsley, *supra* note 6, at 21 (detailing providers' policies and guidance given to law enforcement).

46. *Compare* Commonwealth v. Perry (*Perry I*), No. 1984CR00396, 2021 Mass. Super. LEXIS 49, at *11-12 (Mass. Super. Ct. Apr. 21, 2021) (reasoning tower dump request yields phone numbers, rather than PII), *with* United States v. Walker, No. 2:18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *5-9 (E.D.N.C. July 20, 2020) (listing detailed PII law enforcement requested from providers in court orders), *and* United States v. Rhodes, No. 19-CR-0073-AT-LTW, 2020 U.S. Dist. LEXIS 253307, at *3 (N.D. Ga. June 16, 2020) (stating law enforcement requested personal identifiers for cell phones).

47. *See* Carpenter, 138 S. Ct. at 2217-18. Many providers have set fees to fulfill law enforcement's tower dump requests; for some, cooperating with law enforcement and fulfilling these requests has resulted in revenue to the company. *See* Owsley, *supra* note 6, at 19-20 (detailing varying fees of providers). This revenue acts as an incentive for providers to comply with law enforcement's requests. *See id.* (noting large providers can generate millions of dollars in fees for disclosing phone surveillance).

48. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (discussing law enforcement's past CSLI requests through court orders); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 13-15 (detailing number of CSLI requests providers face, majority without warrant); *see also* Stored Communications Act § 2703(d); Owsley, *supra* note 6, at 2 (suggesting tower dumps relatively routine investigatory technique). In 2015, Verizon received more than 50,000 requests for CSLI and AT&T more than 76,000. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 13-14. T-Mobile, who did not report CSLI requests that year, potentially received a far greater number than its rivals. *See id.* at 14.

49. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (noting Verizon's increased requests for tower dumps); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 13-14. In 2020, T-Mobile received 296,000 CSLI requests, including 12,000 tower dump requests. *See* T-MOBILE, TRANSPARENCY REPORT FOR 2020 6 (2020), https://www.t-mobile.com/news/_admin/uploads/2021/07/2020-Transparency-Report.pdf [https://perma.cc/Y9RG-R34T]. The number of requests T-Mobile faced in 2021 dropped to almost 200,000 CSLI requests, including 9,000 tower dump requests. *See* T-MOBILE, TRANSPARENCY REPORT FOR 2021 6 (2021), https://www.t-mobile.com/news/_admin/uploads/2022/07/2021-Transparency-Report.pdf [https://perma.cc/4L6U-JCFD]. AT&T received over 99,000 CSLI requests in 2020 and 104,000 in 2021, including around 3,000 tower dump requests a year. *See* AT&T, FEBRUARY 2022 TRANSPARENCY REPORT 4 (2022) https://about.att.com/content/dam/csr/2019/transparency/2022/2022-February-Transparency-Report.pdf [https://perma.cc/2ZDM-F6K2]; AT&T, FEBRUARY 2021 TRANSPARENCY REPORT 4 (2021), https://about.att.com/ecms/dam/csr/2019/transparency/2021/2021-February-Report.pdf [https://perma.cc/3AQ-M-FFB8]; AT&T, AUGUST 2021 TRANSPARENCY REPORT 4 (2021), https://about.att.com/ecms/dam/csr/2019/tr-ansparency/2021/20-21-August-Report.pdf [https://perma.cc/AC8Q-BLVZ]; AT&T, AUGUST 2020 TRANSPARENCY REPORT 4 (2020), https://about.att.com/ecms/dam/csr/2019/library/transparency/2020-August-Report.pdf [https://perma.cc/L69P-JVPH].

50. *See supra* note 28 and accompanying text (discussing length of time providers retain CSLI).

tower dump, however, does not just reveal a single user's movements: A tower dump report can reveal thousands—even hundreds of thousands—of users' movements.[51]

The use of a tower dump is well-suited for investigating serial crimes: Law enforcement can cross-reference phone numbers across each crime scene under the assumption an innocent individual is unlikely to be present for multiple crimes.[52] After receiving multiple tower dump reports corresponding to the time and location of the crimes, law enforcement can compare the phone numbers from the reports to narrow down on a suspect device present across numerous scenes.[53] Scholars recognize that a tower dump can also be helpful where law enforcement has identified the crime scene location and timeframe but has not identified the suspect, although the use of a tower dump for identification rests upon the assumption that the suspect carried their cell phone with them.[54] A tower dump, however, yields innocent users alongside guilty users, so its use for criminal investigations may be limited.[55]

A tower dump is distinct from the more precise location information that Google stores, which law enforcement seek through geofence warrants.[56] Google stores location information that is considerably more accurate than CSLI,

---

51. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (noting tower dumps can potentially net thousands of users' location information); Owsley, *supra* note 6, at 18. In one federal case, a tower dump yielded 180 cell phone numbers. *See* Owsley, *supra* note 6, at 18 (providing examples of how many users tower dumps may implicate). In a different federal case, the FBI received over 150,000 cell phone numbers from a single tower dump. *See* LEVINSON-WALDMAN, *supra* note 3, at 2. But tower dumps are usually constrained in that they cover a small area over a short period of time. *See* Kortz & Bavitz, *supra* note 2, at 28 (suggesting tower dumps less revealing than historical CSLI).

52. *See* Owsley, *supra* note 6, at 6 (claiming tower dumps useful for serial crimes because of ability to cross-reference); *Perry I*, No. 1984CR00396, 2021 Mass. Super. LEXIS 49, at *8 (Mass. Super. Ct. Apr. 21, 2021) (articulating unlikelihood innocent individual present across multiple crime scenes).

53. *See James I*, No. 18-cr-216 (SRN/HB), 2018 U.S. Dist. LEXIS 210433, at *6 (D. Minn. Nov. 26, 2018) (describing agent's process to narrow list of suspects by cross-referencing tower dump information); United States v. Rhodes, No. 19-CR-0073-AT-LTW, 2020 U.S. Dist. LEXIS 253307, at *2-3 (N.D. Ga. June 16, 2020) (discussing how government identified suspect of armed robberies); *see also* United States v. Adkinson, 916 F.3d 605, 608 (7th Cir. 2019) (explaining how provider identified robbery suspect through tower dumps and cross-referencing cell phone numbers).

54. *See* Owsley, *supra* note 6, at 22 (discussing United State Department of Justice's advisement on when tower dumps useful); *Rhodes*, 2020 U.S. Dist. LEXIS 253307, at *7 (dismissing Rhodes's argument no connection between robber and cell phone). The court in *Rhodes* stated it could hardly be questioned that it is common for people to keep their cell phones on them. *See Rhodes*, 2020 U.S. Dist. LEXIS 253307, at *7.

55. *See* LEVINSON-WALDMAN, *supra* note 3, at 4 (questioning length of CSLI retention and whether implicated individuals notified). It is unclear just how many agencies retain CSLI for nontargets as this information remains shrouded in secrecy. *See id.* at 4-5.

56. *See In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 739-40 (N.D. Ill. 2020) (emphasizing difference in precision between CSLI and geofence data); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2510 (2021) (distinguishing Google's data from CSLI); Donna Lee Elm, *Geofence Warrants Challenging Digital Dragnets*, 35 CRIM. JUST. 7, 7 (2020) (describing Google's location data far more sensitive than CSLI). A geofence warrant only seeks Google's location data, not CSLI. *See Geofence Warrants and the Fourth Amendment*, *supra*, at 2512-13 (noting Google only known company to respond to geofence warrant).

information gathered through user-enabled features on the cell phone, such as GPS, Wi-Fi, and Bluetooth.[57] Signals from GPS, nearby Wi-Fi networks, and Bluetooth devices provide additional location information and allow for greater precision in estimating the cell phone's location.[58] In contrast, CSLI relies on location information from cell sites alone.[59] Additionally, many cell phone users actively enable such location tracking by Google, whereas cell phone users are not given the option with CSLI.[60]

C. Fourth Amendment Jurisprudence

1. Searches

The Fourth Amendment protects individuals' privacy from unreasonable governmental intrusion.[61] To trigger the warrant requirement of the Fourth Amendment, the government must have engaged in an unreasonable search or seizure.[62] In *Olmstead v. United States*, the Supreme Court first determined a search has occurred when the government has physically trespassed on a constitutionally protected area to obtain information.[63] Over thirty years later, in *Katz v. United States*, the Court amended the meaning of a search to include governmental intrusion to obtain information where one has a reasonable expectation of privacy.[64] Justice Harlan's concurrence established that a reasonable expectation

57. *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (Ecf No. 29) at 7, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-cr-00130) (discussing why Google's location information more precise than other location data).

58. *See id.* (noting combination of user-initiated inputs allow for greater location accuracy).

59. *See id.* (contrasting CSLI and Google's stored location information).

60. *Compare Geofence Warrants and the Fourth Amendment*, *supra* note 56, at 2511 (acknowledging most users permit Google to track their location), *with* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) (discussing involuntary nature of CSLI generation).

61. *See, e.g.*, Katz v. United States, 389 U.S. 347, 350 (1967) (clarifying Fourth Amendment protects against governmental intrusion rather than creating general right to privacy); United States v. Jones, 565 U.S. 400, 404 (2012) (holding physical intrusion on Jones's car considered search under Fourth Amendment); *Carpenter*, 138 S. Ct. at 2213 (noting Fourth Amendment protects against intrusion where one has reasonable expectation of privacy). The Supreme Court noted the Fourth Amendment's protections go further than just individual privacy, "often having nothing to do with privacy at all." *See Katz*, 389 U.S. at 350.

62. *See* U.S. CONST. amend. IV; *Carpenter*, 138 S. Ct. at 2213 (detailing expansion of Fourth Amendment's protections).

63. *See* 277 U.S. 438, 466 (1928) (finding no search where no government physical intrusion), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); *see also Jones*, 565 U.S. at 407 (reaffirming government physical intrusion may constitute search). A constitutionally protected area simply refers to an area the courts have determined is protected by the Constitution. *See Olmstead*, 277 U.S. at 466 (explaining home and curtilage of home constitutionally protected areas).

64. *See Katz*, 389 U.S. at 353 (concluding use of electronic listening device on phone booth violated Katz's justifiable expectation of privacy). The Supreme Court explained the Fourth Amendment "protects people, not places," allowing constitutional protection to extend to public areas one seeks to preserve as private. *See id.* at 351 (clarifying issue presented in case). Following this rationale, the Court concluded the Fourth Amendment protects one who enters a public phone booth, closes the door, and pays the fee from unreasonable intrusion on their conversations—even though the government could see inside the booth. *See id.* at 352.

of privacy is twofold, requiring a subjective expectation of privacy and an objective expectation of privacy that society would recognize as reasonable.[65]

While the Supreme Court has amended the meaning of a search, it has not justified all expectations of privacy as objectively reasonable.[66] In its decisions in *United States v. Miller* and *Smith v. Maryland*, the Court created a large Fourth Amendment exception with the third-party doctrine.[67] The third-party doctrine established that the Fourth Amendment does not protect information voluntarily conveyed to a third party because there is no objectively reasonable expectation of privacy; consequently, the government may request that information without a warrant.[68] The Court reasoned that one assumes the risk that information conveyed to third parties may be shared, even when one conveys it with the belief the third party will not share that information.[69]

2. Warrant Requirements

a. Probable Cause

When the Fourth Amendment requires a warrant, law enforcement must obtain a warrant that is based upon probable cause before they can search.[70] Probable cause does not have a clear threshold; rather, it is a fluid concept that turns upon probabilities of criminal activity under the factual circumstances.[71] A probability of criminal activity is sufficient to issue a warrant when it allows the

65. *Id.* at 361 (Harlan, J., concurring) (setting forth two-part test in determining whether reasonable expectation of privacy exists). While not explicitly adopted in the majority opinion, Justice Harlan's two-prong test became the approach the Supreme Court utilizes to this day. *See, e.g.*, *Jones*, 565 U.S. at 405 (acknowledging application of Justice Harlan's test to later cases); Smith v. Maryland, 442 U.S. 735, 740-41 (1979) (applying two-part analysis to facts of case).

66. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983) (holding no reasonable expectation of privacy for cars traveling on public roads, meaning no search); United States v. Miller, 425 U.S. 435, 440 (1976) (determining no search occurred because no justifiable expectation of privacy in bank records); *Smith*, 442 U.S. at 745 (holding no legitimate expectation of privacy in phone numbers dialed).

67. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (tracing third-party doctrine roots back to *Miller* and *Smith*); *Miller*, 425 U.S. at 443 (reiterating notion of no reasonable expectation of privacy in information conveyed to third parties); *Smith*, 442 U.S. at 744 (analyzing Smith's claim under third-party doctrine established in *Miller*).

68. *See Miller*, 425 U.S. at 443 (articulating extent of third-party doctrine); *Smith*, 442 U.S. at 744 (reaffirming no legitimate expectation of privacy in information given to third parties).

69. *See Miller*, 425 U.S. at 443 (discussing one assumes risk when sharing information with another party); *Smith*, 442 U.S. at 745 (reasoning Smith assumed risk provider would divulge voluntarily conveyed information to law enforcement).

70. *See, e.g.*, U.S. CONST. amend. IV (requiring probable cause for warrant to protect against unreasonable searches and seizures); *Carpenter*, 138 S. Ct. at 2213 (detailing Fourth Amendment's search doctrine and when warrant required); Katz v. United States, 389 U.S. 347, 357 (1967) (discussing unlawfulness of warrantless searches).

71. *See* Illinois v. Gates, 462 U.S. 213, 232 (1983) (describing probable cause standard); *James II*, 3 F.4th 1102, 1105-06 (8th Cir. 2021) (dismissing James's lack of probable cause argument because probable cause deals with probabilities, not certainties).

magistrate to form a substantial basis that a search would reveal evidence of a crime.[72] Courts determine whether probable cause exists through a totality of the circumstances—a consideration of all relevant circumstances.[73] The Supreme Court has articulated the probable cause determination is a "practical, common-sense judgment."[74]

b. Particularity

The Fourth Amendment expressly requires warrants to "particularly describe[] the place to be searched, and the persons or things to be seized."[75] One purpose of the particularity requirement is to prevent general search warrants.[76] Particularity also assures the individual being searched or seized that there is a need for the search or seizure, the executing officer has the authority to search or seize, and the officer's power in conducting the search and seizure is limited.[77] The particularity requirement extends to people; thus, a search or seizure of a person requires probable cause particular to the targeted individual.[78] Some courts have articulated, however, that the required specificity for the warrant may be flexible depending on the circumstances.[79] Courts have determined a warrant

72. *See Gates*, 462 U.S. at 236 (reaffirming totality-of-circumstances standard for probable cause determinations).

73. *See id.* at 230-31 (abandoning previous technical approach in favor of flexible totality-of-circumstances test).

74. *See id.* at 244 (discussing factual circumstances may not have satisfied previous test, but sufficient under totality approach).

75. U.S. CONST. amend. IV.

76. *See* Groh v. Ramirez, 540 U.S. 551, 561 (2004). General warrants specify only a criminal offense, leaving law enforcement with unconstrained discretion as to whom and what to search and seize. *See* Stanford v. Texas, 379 U.S. 476, 481 (1965) (providing history of general warrants and their prohibition); *Geofence Warrants and the Fourth Amendment*, *supra* note 56, at 2518 (defining general warrants). The Fourth Amendment expressly prohibits general warrants by requiring a particular description of the things and people to be searched and seized. *See* U.S. CONST. amend. IV (articulating particularity requirement before warrant issued); Marron v. United States, 275 U.S. 192, 196 (1927) (explaining particularity requirement constrains law enforcement's discretion); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (reiterating Fourth Amendment's ability to combat general warrants through particularity requirement).

77. *See Groh*, 540 U.S. at 561 (explaining multiple purposes served by particularity requirement).

78. *See* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (stressing one cannot undercut requirement by pointing to probable cause to search or seize another); Marks v. Clarke, 102 F.3d 1012, 1028 (9th Cir. 1996) (affirming invalidity of warrant for "any persons on the premises" due to lack of particularity).

79. *See* United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982) (asserting "practical margin of flexibility" for particularity requirement universally recognized); United States v. Martin, 866 F.2d 972, 977 (8th Cir. 1989) (stating required degree of specificity possibly flexible under circumstances); United States v. Young, 745 F.2d 733, 759 (2d Cir. 1984) (noting lesser specificity tolerated where law enforcement has done best it could do under circumstances); *James I*, No. 18-cr-216 (SRN/HB), 2018 U.S. Dist. LEXIS 210433, at *9 (D. Minn. Nov. 26, 2018) (setting forth flexible legal standard for particularity requirement); *see also* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 4.5(e) (6th ed. 2021) (discussing scenarios where lesser specificity in warrant still sufficient). *But see Marron*, 275 U.S. at 196 (detailing how particularity requirement leaves nothing to law enforcement's discretion); *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (finding geographically and time-tailored search insufficient to meet particularity requirement). If courts read *Marron* literally, few warrants would satisfy the particularity requirement. *See* LAFAVE, *supra*, § 4.6(a), at 1. Consequently, courts have tended to interpret the particularity

description is sufficiently particularized "if it is as specific as the circumstances and nature of activity under investigation permit."[80]

An all-person warrant specifies the place to be searched but does not name an individual, allowing law enforcement to search all those on the premises.[81] Despite the flexibility of the particularity requirement, these warrants will not typically satisfy this requirement.[82] All-person warrants will only satisfy the particularity requirement where there is probable cause to believe that *all* those present during the warrant's execution are participating in the specified criminal activity.[83] Therefore, law enforcement could utilize an all-person warrant for locations exclusively dedicated to criminal activity, such as a barn used as an methamphetamine lab or an apartment as a drug den.[84]

D. Stored Communications Act

The Fourth Amendment requires law enforcement to obtain a warrant to conduct a search, but numerous courts have concluded that law enforcement requesting CSLI does not constitute a search.[85] Prior to the Supreme Court's decision in *Carpenter*, the Fourth Amendment did not protect CSLI and providers did not have to require a warrant for disclosure.[86] Instead, law enforcement could

---

requirement more flexibly. *See, e.g.*, *Wuagneux*, 683 F.2d at 1349; *Martin*, 866 F.2d at 977; *Young*, 745 F.2d at 759.

80. *See, e.g.*, *Wuagneux*, 683 F.2d at 1349 (articulating when warrant description suffices); *Martin*, 866 F.2d at 977 (applying standard from *Wuagneux* when analyzing description of search warrant); *Young*, 745 F.2d at 759 (supporting idea particularity flexible depending on what circumstances allow). For example, a court upheld a search warrant listing money and "other evidence" to be seized from suspects of a heroin enterprise; it reasoned "other evidence" following "money" constrained what law enforcement could seize to manifestations of wealth. *See Young*, 745 F.2d at 759-60 (concluding agents could not give more narrow description). In another case, the court upheld a search warrant that included vague terms such as "kickback" because of the complex financial transactions and various types of fraud involved. *See Wuagneux*, 683 F.2d at 1349 (allowing less specificity in warrant for crimes involving complex financial transactions and widespread fraud).

81. *See Marks*, 102 F.3d at 1029 (outlining all-person warrant and its inherent issues).

82. *See id.* (explaining warrants specifying only location of search does not satisfy particularized probable cause requirement); Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004) (affirming when all-person warrant constitutional).

83. *See Marks*, 102 F.3d at 1029 (explaining all-person warrant appropriate for locales "dedicated exclusively to criminal activity"); *Owens*, 372 F.3d at 276 (affirming when all-person warrant constitutional).

84. *See* Marks v. Clarke, 102 F.3d 1012, 1029 (9th Cir. 1996) (describing limited circumstances when all-person warrant constitutional).

85. *See* United States v. Hammond, 996 F.3d 374, 387 (7th Cir. 2021) (hesitating to extend protection to real-time CSLI); United States v. Adkinson, 916 F.3d 605, 611 (7th Cir. 2019) (denying motion to suppress CSLI because *Carpenter* excluded tower dumps from holding); United States v. Walker, No. 18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *22-23 (E.D.N.C. July 20, 2020) (finding no reason to attach Fourth Amendment protections to tower dumps); United States v. Rhodes, No. 19-CR-0073-AT-LTW, 2020 U.S. Dist. LEXIS 253-307, at *6 (N.D. Ga. June 16, 2020) (concluding tower dumps pose lesser privacy concerns). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding legitimate expectation of privacy in historical CSLI, constituting search).

86. *See* Hoover, *supra* note 22, at 761 (explaining each circuit court to address CSLI determined it did not constitute search); LEVINSON-WALDMAN, *supra* note 3, at 2 (declaring warrant not required for CSLI before *Carpenter*).

obtain—and often chose to obtain—a court order under the SCA.[87] In enacting the SCA, Congress criminalized unauthorized access to records or contents of electronic communications, thereby requiring providers to prevent disclosure of PII and CSLI unless there is a valid court order granting third-party access.[88] In contrast to the Fourth Amendment's probable cause requirement, the SCA only requires law enforcement to demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[89] This reasonable suspicion standard is much lower than that of probable cause—giving law enforcement easy access to CSLI.[90]

E. CSLI Jurisprudence

1. Carpenter v. United States

In *Carpenter*, law enforcement arrested four men suspected of robbing multiple Radio Shack and T-Mobile stores in Ohio and Michigan.[91] The suspects provided the FBI with phone numbers of some of their accomplices, and the FBI used the suspects' call records to identify additional numbers connected to the crimes.[92] Based on the suspects' call records, prosecutors sought court orders under the SCA for the cell phone records of several suspects, including that of defendant Timothy Carpenter.[93] A federal magistrate issued two court orders directing Carpenter's providers to disclose his CSLI.[94] The first order produced records for 127 days and the second for two days, resulting in 12,898 location

87. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (stating law enforcement generally obtained CSLI under SCA prior to *Carpenter* decision); Stored Communications Act, 18 U.S.C § 2703(d) (allowing access to CSLI and PII if low standard of specific and articulable facts met). Congress enacted the SCA in 1986 to protect users' privacy by criminalizing unauthorized access to content or records of electronic communications. *See* United States v. Appelbaum (*In re* United States), 707 F.3d 283, 286-87 (4th Cir. 2013) (outlining purpose of SCA passage). The SCA allows law enforcement to compel providers to disclose the content and records of the user's electronic communications. *See id.* at 287 (discussing process of obtaining information under SCA).

88. *See Appelbaum*, 707 F.3d at 286-87 (explaining requirements under SCA).

89. Stored Communications Act § 2703(d) (setting forth court order requirement of "specific and articulable facts" to gather CSLI).

90. *See Carpenter*, 138 S. Ct. at 2221 (comparing SCA standard to probable cause standard); Commonwealth v. Augustine, 4 N.E.3d 846, 852 (Mass. 2014) (asserting SCA standard lower than probable cause standard); Stored Communications Act § 2703(d) (requiring only "specific and articulable facts showing . . . information sought, [is] relevant and material"); Amanda Regan, Note, *Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause Is Not Necessary for Cell Tower Dumps*, 43 HOFSTRA L. REV. 1189, 1197 (2015) (supporting lower SCA standard for tower dumps). The reasonable suspicion standard merely requires the record to be relevant and material to an ongoing investigation, whereas the probable cause standard requires enough evidence to believe an offense has been, is being, or will be committed and the record sought will produce evidence of that offense or will aid in apprehending the suspect. *See Augustine*, 4 N.E.3d at 873-74 (Gants, J., dissenting).

91. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (laying out factual circumstances of case).

92. *Id.* (explaining FBI agents tried to identify phone numbers called around time of crime).

93. *Id.* (discussing court orders magistrate judge granted which covered four-month period).

94. *Id.*

points that cataloged Carpenter's movements.[95] Carpenter moved to suppress his CSLI, claiming he had a right to privacy in his movements.[96] The lower court denied his motion based on the third-party doctrine, with the Sixth Circuit affirming the denial.[97]

The Supreme Court granted certiorari and addressed whether government access to a user's historical CSLI constitutes a search under the Fourth Amendment.[98] In the majority opinion, Chief Justice Roberts first noted the historical understanding of a search during the Fourth Amendment's adoption informed the analysis.[99] He then explained the CSLI at issue lies between two lines of precedent: an individual's expectation of privacy in their location and movements and an individual's lack of expectation of privacy in information they have conveyed to a third party.[100] Chief Justice Roberts noted many similarities between CSLI and the twenty-eight day GPS tracking held to be a search in *United States v. Jones*—in both instances, the information was *detailed*, *encyclopedic*, and *effortlessly compiled*.[101] At the same time, he recognized individuals share CSLI with their providers, which implicates the third-party doctrine.[102]

In its landmark decision, the Court ultimately declined to extend the third-party doctrine to CSLI, concluding CSLI is unique because of its comprehensive and infallible nature.[103] It held that obtaining historical CSLI is a search under the Fourth Amendment because one maintains an expectation of privacy in this information; thus, the government may not request seven days or more of

95. *Carpenter*, 138 S. Ct. at 2212 (noting average of 101 data points per day).

96. *Id.*

97. Carpenter v. United States, 138 S. Ct. 2206, 2212-13 (2018) (discussing lower court's finding of no reasonable expectation of privacy because Carpenter shared his CSLI).

98. *See id.* at 2211 (posing question addressed in case).

99. *See id.* at 2214 (articulating commitment to preserving historical understanding of privacy).

100. *See id*. at 2214-15 (explaining issue did not neatly fall under existing precedent). Chief Justice Roberts first addressed the Court's previous decision in *Knotts*, where it held the government's use of a "beeper" to track a vehicle on public roads did not constitute a search. *See id.* at 2215; *see also* United States v. Knotts, 460 U.S. 276, 285 (1983). The *Knotts* Court reasoned one traveling on public roads does not have an expectation of privacy in their movements because they have voluntarily conveyed their movements to whomever wanted to look; nevertheless, the Court distinguished this type of limited tracking from twenty-four-hour surveillance. *See Knotts*, 460 U.S. at 283-84 (reserving question of constitutionality of twenty-four-hour surveillance for when such "dragnet" surveillance occurs). Chief Justice Roberts then delved into the Court's previous decision in *Jones*, where it determined twenty-eight days of GPS monitoring constituted a search because of the government's physical trespass in placing the GPS on Jones's car. *See Carpenter*, 138 S. Ct. at 2215 (noting concurring opinion concluded long-term GPS monitoring infringed on privacy expectation, regardless of public disclosure); *see also* United States v. Jones, 565 U.S. 400, 404 (2012). Finally, Chief Justice Roberts addressed the Court's second set of decisions involving the third-party doctrine that rested on the rationale that individuals assume the risk of disclosure when voluntarily sharing information with third parties. *See Carpenter*, 138 S. Ct. at 2216 (questioning whether this logic extends to CSLI at issue).

101. *See Carpenter*, 138 S. Ct. at 2216 (comparing CSLI qualities with long-term GPS monitoring qualities).

102. *See id.* (explaining one assumes risk when sharing information with third parties).

103. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (acknowledging Fourth Amendment protections can extend to public places).

historical CSLI under the SCA and must get a warrant.[104] In so holding, the Court focused on historical CSLI's ability to provide a detailed, all-encompassing recording of the user's location and an intimate view into their life.[105] The Court determined providers' collection of CSLI presents even greater privacy concerns than the GPS tracking in *Jones*—as a cell phone "faithfully follows its owner beyond public thoroughfares" and provides law enforcement access to location information that would otherwise be unknowable.[106] Further, it suggested that users do not voluntarily share CSLI in any meaningful sense because a cell phone can create CSLI without any affirmative act of the user beyond turning the cell phone on.[107]

In concluding that obtaining historical CSLI qualifies as a search under the Fourth Amendment and that law enforcement is required to secure a warrant, the Court was careful to iterate its decision was narrow.[108] The Court's decision limited protection of historical CSLI to requests for seven days or more of location data.[109] The Court also declined to express a view on either real-time CSLI or tower dumps and noted the decision did not disturb the application of the third-party doctrine to circumstances beyond historical CSLI.[110]

2. Tower Dumps Post-Carpenter

Following the Supreme Court's decision in *Carpenter*, defendants have repeatedly argued Fourth Amendment protections for historical CSLI should apply

104. *See id.* at 2221 (comparing lowered showing required under SCA with heightened probable cause showing). The Court concluded law enforcement needs a warrant when requesting seven days or more of a user's historical CSLI but provided no reason for the line being set at seven days. *See id.* at 2217 n.3 (clarifying when Fourth Amendment triggered for historical CSLI records).

105. *See id.* at 2217 (analyzing privacy concerns implicated through historical CSLI collection). Historical CSLI does not just reveal one's movements but also deeply personal information, including one's "familial, political, professional, religious, and sexual associations" though their movements. *See id.* (quoting Justice Sotomayor's previous opinion in *United States v. Jones*); *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).

106. *See Carpenter*, 138 S. Ct. at 2218 (contrasting previously limited surveillance in *Knotts* and *Jones* with "near perfect" CSLI surveillance). The Court explained that law enforcement's attempts to reconstruct an individual's movements were previously limited to available surveillance, but now, access to CSLI affords law enforcement the ability to retrace an individual's historic movements spanning back years. *See id.* It further distinguished the GPS tracking used in *Jones* that implicated one person from CSLI that implicates every cell phone user. *See id.* (noting law enforcement need not even know particular suspect in advance of search with CSLI).

107. *See Carpenter*, 138 S. Ct. at 2220 (outlining why third-party doctrine reasoning of voluntary exposure fails when it comes to CSLI). Chief Justice Roberts reasoned the involuntary nature of CSLI transmission means users do not assume the risk of disclosure of their comprehensive movements. *See id.* (declining to extend third-party doctrine to CSLI).

108. *See id.* (refusing to express view on issues not before it).

109. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018) (rejecting to determine whether government may obtain CSLI for lesser period without implicating Fourth Amendment). The seven-day cutoff sparked Justice Gorsuch to question how tower dumps could survive under the Court's test when historical CSLI could not. *See id.* at 2266-67 (Gorsuch, J., dissenting) (asking why tower dumps not classic example of "too permeating police surveillance" under *Katz* analysis).

110. *See id.* at 2220 (majority opinion) (explaining Court's narrow decision).

to tower dumps.[111] These arguments, however, have remained largely unsuccessful in court.[112] Multiple courts have reasoned tower dumps simply do not implicate the privacy concerns present in historical CSLI.[113] A tower dump covers a limited area and time, whereas historical CSLI reveals the intimacies of an individual's life through an "all-encompassing" catalogue of movement over a long period.[114] Courts have further noted *Carpenter* explicitly excluded tower dumps from the narrow decision and have declined to extend Fourth Amendment protections on that basis.[115]

Defendants have further argued a tower dump warrant is not sufficiently particularized, but this argument has not fared any better with the courts.[116] The Eighth Circuit, for example, reasoned a geographically—and temporally—constrained tower dump warrant was sufficiently particularized because these limitations "eliminate[d] any confusion about what the investigators could search."[117] Multiple state courts reached the same conclusion, similarly citing

111. *See* United States v. Adkinson, 916 F.3d 605, 610 (7th Cir. 2019) (analyzing Adkinson's challenge of warrantless tower dump); United States v. Walker, No. 18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *15 (E.D.N.C. July 20, 2020) (addressing Walker's argument Fourth Amendment protects against warrantless tower dumps); United States v. Rhodes, No. 19-CR-0073-AT-LTW, 2020 U.S. Dist. LEXIS 253307, at *3-4 (N.D. Ga. June 16, 2020) (outlining Rhodes's argument of no logical justification to not provide protection for tower dumps); State v. Hudson, No. 1809009750, 2021 Del. Super. LEXIS 670, at *20-22 (Del. Super. Ct. Nov. 23, 2021) (rejecting Hudson's claim *Carpenter* protections apply to tower dumps); *see also* Mary Madden, *Public Perceptions of Privacy and Security in the Post*-Snowden *Era*, PEW RSCH. CTR. (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ [https://perma.cc/A2LY-NUGM] (suggesting majority of cell phone users have subjective expectation of privacy in location).

112. *See Adkinson*, 916 F.3d at 610-11 (dismissing Adkinson's argument against warrantless tower dumps); *Walker*, 2020 U.S. Dist. LEXIS 126774, at *23 (rejecting Fourth Amendment protection to tower dump CSLI); *Rhodes*, 2020 U.S. Dist. LEXIS 253307, at *6 (concluding warrant not required for tower dump); *Hudson*, 2021 Del. Super. LEXIS 670, at *21-22 (outlining rationale behind denial of Hudson's argument).

113. *See Walker*, 2020 U.S. Dist. LEXIS 126774, at *21-22 (distinguishing comprehensive catalogue of movement in historical CSLI and limited movement revealed by tower dump); *Rhodes*, 2020 U.S. Dist. LEXIS 253307, at *6 (comparing precise and extended historical CSLI with limited showing of prior location under tower dump).

114. *See Walker*, 2020 U.S. Dist. LEXIS 126774, at *21-22 (finding same privacy concerns of historical CSLI not implicated by tower dumps); *Perry I*, No. 1984CR00396, 2021 Mass. Super. LEXIS 49, at *10-11 (Mass. Super. Ct. Apr. 21, 2021) (distinguishing limited surveillance of tower dumps from revealing historical CSLI). *Compare supra* note 42 (describing tower dumps and lower level of intrusion on individual), *with supra* note 105 (discussing deeply-revealing nature of historical CSLI).

115. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (declining to provide view on tower dumps); *Adkinson*, 916 F.3d at 611 (clarifying *Carpenter* "did not invalidate warrantless tower dumps"); *Walker*, 2020 U.S. Dist. LEXIS 126774, at *21-23 (noting Supreme Court explicitly declined to express view on tower dumps); *Rhodes*, 2020 U.S. Dist. LEXIS 253307, at *4, *6 (rejecting argument *Carpenter*'s limited holding provides protection to tower dumps); *Hudson*, 2021 Del. Super. LEXIS 670, at *21-22 (reasoning *Carpenter* does not apply to tower dumps based on opinion's express language); People v. Root, No. 346164, 2020 Mich. App. LEXIS 2712, at *15-16 (Mich. Ct. App. Apr. 9, 2020) (refusing to hold warrantless tower dumps inappropriate).

116. *See James II*, 3 F.4th 1102, 1104, 1106 (8th Cir. 2021) (discussing James's claim); *Perry I*, 2021 Mass. Super. LEXIS 49, *13 (finding Perry's search warrant had enough particularity).

117. *See James II*, 3 F.4th at 1106 (agreeing with lower court's reasoning).

the tower dump warrant's limited scope in time and location.[118] The Massachusetts Suffolk Superior Court acknowledged a tower dump warrant was broad in the sense that it captured extensive information about innocent individuals, but ultimately found it to be sufficiently particularized because there was not a less intrusive way to identify the suspects.[119]

3. State CSLI Laws

Despite courts' repeated refusal to extend *Carpenter*'s protections to other types of CSLI, a growing number of state legislatures are requiring a warrant to obtain any kind of location information from a third party.[120] These states require law enforcement to get a warrant for any CSLI—historical, real-time, or tower dump—affording greater protection than *Carpenter*.[121] Colorado, Illinois, Maine, Minnesota, Montana, New Hampshire, Rhode Island, Tennessee, Utah, Vermont, and Wisconsin have all passed such legislation.[122] Indiana, Maryland, Texas, and Virginia have passed legislation requiring a warrant for real-time CSLI only.[123]

Conversely, Alabama, Arizona, Florida, and New Jersey have passed legislation expressly allowing law enforcement to obtain CSLI without a warrant.[124] Legislation in these states references or mirrors the language of the SCA, allowing law enforcement to obtain CSLI through a court order.[125] Law enforcement must show "specific and articulable facts" demonstrating the information is

118. *See* State v. Hudson, No. 1809009750, 2021 Del. Super. LEXIS 670, at *24 (Del. Super. Ct. Nov. 23, 2021) (distinguishing unparticularized warrant not limiting search with warrant containing specific time frame); *Perry I*, 2021 Mass. Super. LEXIS 49, at *12-13 (reasoning warrant particularized).

119. *See Perry I*, 2021 Mass. Super. LEXIS 49, at *12-13 (suggesting particularity requirement flexible depending upon crime under investigation).

120. *See* COLO. REV. STAT. § 16-3-303.5 (2023); 725 ILL. COMP. STAT. ANN. 168/10 (West 2022); ME. REV. STAT. ANN. tit. 16, § 648 (2022); MINN. STAT. ANN. § 626A.42 (West 2023); MONT. CODE ANN. § 46-5-110 (West 2022); N.H. REV. STAT. ANN. § 644-A:2 (2022); 12 R.I. GEN. LAWS § 12-32-2 (2022); TENN. CODE ANN. § 39-13-610 (2022); UTAH CODE ANN. § 77-23c-102 (LexisNexis 2022); VT. STAT. ANN. tit. 13, § 8102 (2022); WIS. STAT. ANN. § 968.375 (West 2022) (allowing disclosure of CSLI by warrant *or* subpoena supported by probable cause).

121. *Compare supra* note 120 (showing states requiring warrant for *all* location information), *with* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (requiring warrant for *only* historical CSLI).

122. *See supra* note 120 (listing states requiring warrant for any location information).

123. *See* IND. CODE ANN. § 35-33-5-12 (West 2022) (limiting real-time tracking by requiring warrant); MD. CODE ANN., CRIM. PROC. § 1-203.1 (LexisNexis 2022) (using warrant standard to require court order for real-time CSLI); TEX. CODE CRIM. PROC. ANN. art. 18B.321 (West 2023) (suggesting warrant required for prospective CSLI); TEX. CODE CRIM. PROC. ANN. art. 18B.352 (West 2023) (giving law enforcement access to electronically-stored customer information by court order); VA. CODE ANN. § 19.2-70.3 (2022) (requiring warrant for real-time CSLI with certain crime exceptions).

124. *See* ALA. CODE § 15-5-40 (2022); ARIZ. REV. STAT. § 13-3016(c) (LexisNexis 2022); FLA. STAT. ANN. § 934.23 (West 2022); N.J. STAT. ANN. § 2A:156A-29 (West 2023).

125. *Compare supra* note 124 (cataloging states with legislation similar to SCA standard), *with* Stored Communications Act, 18 U.S.C § 2703(d) (setting forth SCA standard).

"relevant and material" to the criminal investigation—a lower standard than probable cause.[126]

A few states that have not passed legislation have instead addressed CSLI through case law.[127] The Ohio Second District Court of Appeals mandates a warrant for requesting even one day of a user's historical CSLI.[128] The Massachusetts Supreme Judicial Court (SJC), meanwhile, mandates a warrant when law enforcement requests over six hours of historical CSLI.[129] In its recent decision addressing cell tower dumps, the SJC held that a warrant is also required if law enforcement seeks reports spanning across multiple days.[130] The SJC further held the Massachusetts Constitution mandates a warrant for real-time CSLI.[131] The Oregon Court of Appeals reached a similar conclusion, determining individuals maintain a reasonable expectation of privacy in their real-time CSLI under the Oregon Constitution.[132] The Washington State Supreme Court also held that requesting real-time CSLI constitutes a search under both its state constitution and the Fourth Amendment.[133] The Kentucky Court of Appeals similarly held that one has a legitimate expectation of privacy in real-time CSLI under the Fourth Amendment.[134]

---

126. *See supra* note 90 (comparing heightened probable cause standard to lower SCA standard).

127. *See* LEVINSON-WALDMAN, *supra* note 3, at 4 (explaining only some states passed legislation addressing CSLI); *infra* notes 129-134 and accompanying text (detailing state case law concerning various types of CSLI protections).

128. *See* State v. Snowden, 140 N.E.3d 1112, 1126 (Ohio Ct. App. 2019) (contending no rationale for not considering one day of CSLI search). In its opinion, the court concluded law enforcement needed a warrant to "ping" the defendant's cell phone and obtain their real-time CSLI. *See id.* at 1126-27 (rejecting argument *Carpenter* limited warrant requirement to seven days of CSLI).

129. *See* Commonwealth v. Augustine, 4 N.E.3d 846, 866 n.37 (Mass. 2014) (indicating warrant required for over six hours of CSLI under state constitution); MASS. CONST. pt. 1, art. 14 (providing greater protection for Massachusetts citizens against unreasonable searches and seizures).

130. *See Perry II*, 184 N.E.3d 745, 763 (Mass. 2022) (reasoning tower dumps across multiple days reveal pattern of activity); MASS. CONST. pt. 1, art. 14 (granting freedom from unreasonable searches and seizures).

131. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1188 (Mass. 2019) (concluding real-time CSLI amounts to search under article 14); MASS. CONST. pt. 1, art. 14 (protecting against unreasonable searches). The SJC reasoned that law enforcement's use of real-time CSLI is highly intrusive and reveals data that "would . . . not otherwise be collected and retained by the service provider." *See Almonor*, 120 N.E.3d at 1193 (reasoning cell phone "ping" constitutes search). Thus, the SJC concluded that there is a reasonable expectation of privacy in real-time CSLI as society would not reasonably expect law enforcement to "be able to secretly manipulate our personal cell phones for any purpose, let alone for the purpose of transmitting our personal location." *See id.* at 1193-94.

132. *See* State v. Hawthorne, 504 P.3d 1185, 1190 (Or. Ct. App. 2021) (concluding trial court did not err in finding expectation of privacy in real-time CSLI); OR. CONST. art. I, § 9 (prohibiting unreasonable searches and seizures).

133. *See* State v. Muhammad, 451 P.3d 1060, 1068-69 (Wash. 2019) (analyzing constitutional privacy protections afforded to CSLI); WASH. CONST. art. I, § 7 (prohibiting invasion of home and private affairs without legal authority); U.S. CONST. amend. IV.

134. *See* Reed v. Commonwealth, No. 2018-CA-001574-MR, 2020 Ky. App. Unpub. LEXIS 656, at *2 (Ky. Ct. App. Feb. 7, 2020) (concluding acquiring real-time CSLI triggers Fourth Amendment protections); *see also* U.S. CONST. amend. IV.

III. ANALYSIS

A. Cell Phone Users Maintain a Reasonable Expectation of Privacy in Their CSLI

Although *Carpenter* excluded tower dumps from its holding, a tower dump intrudes on a user's reasonable expectation of privacy and should constitute a search when law enforcement requests CSLI or PII.[135] While tower dump CSLI contains less location data from one user than does historical CSLI, it can be equally as revealing as historical CSLI.[136] Cell phones follow users beyond public areas, thereby creating a detailed record of their private movements that can reveal "familial, political, professional, religious, and sexual associations," even over short periods.[137] CSLI, therefore, expands law enforcement's surveillance capabilities by providing access to historical information of *every* cell phone user that law enforcement would otherwise be unable to obtain.[138] CSLI alone can reveal these private details about a user, but the intrusion of privacy is much greater with PII because the location information is then linked to a named user.[139] After all, there is a big difference between knowing what cell phone number was at the crime scene and knowing that Jane Smith was there.[140]

135. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218, 2220-21 (2018) (outlining vast capabilities of CSLI in surveillance); *Perry II*, 184 N.E.3d at 759-60 (discussing intimate nature of information CSLI conveys); Lux, *supra* note 8, at 113 (stating tower dumps should constitute search under Supreme Court precedent); Lal, *supra* note 3, at 544 (asserting tower dumps violate individuals' expectation of privacy); *see also* Madden, *supra* note 111 (outlining location information considered more private than contents of text messages for majority of respondents). The SJC concluded Massachusetts was prepared to recognize a reasonable expectation of privacy in CSLI when law enforcement requests tower dumps across multiple days. *Perry II*, 184 N.E.3d at 452-53 (reasoning tower dumps spanning multiple days reveals pattern of activity, implicating greater privacy concerns).

136. *See* Lal, *supra* note 3, at 538 (explaining short-term surveillance could reveal private information like attendance at religious or political gathering); Owsley, *supra* note 6, at 11-13 (suggesting tower dumps protected by Fourth Amendment). *But see* Kortz & Bavitz, *supra* note 2, at 29 (asserting tower dumps arguably less invasive for individuals than historical CSLI).

137. *See Carpenter*, 138 S. Ct. at 2217 (discussing consequence of cell phones going beyond public thoroughfares); *Perry II*, 184 N.E.3d 745, 762 (Mass. 2022) (noting CSLI can easily locate people in private areas). With advancing cell site technology capable of pinning a user's location down to the floor of a building, CSLI can reveal previously-unknowable, intimate details about *all* cell phone users in any areas with cell sites nearby. *See Perry II*, 184 N.E.3d at 753, 762.

138. *See Carpenter*, 138 S. Ct. at 2217-18 (describing privacy concerns inherent in CSLI); Lux, *supra* note 8, at 114 (reasoning law enforcement traditionally would have to rely on real-time tracking or town snoop). Tower dumps can implicate hundreds, if not hundreds of thousands, of users; law enforcement would be utterly incapable of precisely cataloguing all these users' past movements through available surveillance records and individual memory. *See* Lux, *supra* note 8, at 114.

139. *See Perry II*, 184 N.E.3d at 759.

140. *See id.* (highlighting implication when user's identity tied to their CSLI). Restricting law enforcement's requests to only phone numbers, however, may still allow law enforcement to easily identify an individual user. *See Perry I*, No. 146144, 1984CR00396, 2021 Mass. Super. LEXIS 49, at *4 (Mass. Super. Ct. Apr. 21, 2021) (noting law enforcement learned defendant's identity from previously obtaining his phone number in unrelated incident).

The shorter period of surveillance involved in a tower dump should not bar the recognition of an expectation of privacy.[141] The Supreme Court has reiterated concern over technological advances shrinking the degree of privacy that was present at the Fourth Amendment's founding, not just the length of the surveillance.[142] CSLI shrinks the degree of privacy guaranteed to individuals by continuously generating a precise and detailed historical record of every cell phone user's movements.[143] Cell phones can generate CSLI as frequently as every seven seconds and this data is continuously being compiled, which some providers store indefinitely.[144] Access to CSLI records exists contrary to society's expectation that law enforcement cannot catalogue a person's movements for long periods, let alone the movements of every cell phone user.[145]

The third-party doctrine should not be applicable to tower dumps for the same reasons given by the Supreme Court in *Carpenter*.[146] While tower dump CSLI is arguably less invasive than historical CSLI, it is more invasive than the limited technology at issue in *Smith*.[147] Additionally, CSLI contained in a tower dump is shared with providers in the exact same manner as historical CSLI: without any true voluntariness on the part of the user.[148] Once a user powers on a cell phone, which is essential in modern life, it begins to continuously create CSLI that providers store.[149]

---

141. *See* Lux, *supra* note 8, at 113 (asserting Supreme Court also concerned with protecting founding privacy rights against encroaching technology).

142. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (reiterating support of preserving individual privacy); Kyllo v. United States, 533 U.S. 27, 33-35 (2001) (concluding brief thermal imaging of home amounted to search); United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (acknowledging great privacy concerns involved in even short-term surveillance); Lux, *supra* note 8, at 113 (analyzing users' reasonable expectation of privacy regarding tower dumps).

143. *See Carpenter*, 138 S. Ct. at 2217-18 (discussing privacy implications of detailed CSLI records); Lux, *supra* note 8, at 114 (explaining intrusive nature of CSLI data).

144. *See supra* notes 26, 28 (providing technical overview of CSLI).

145. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2217 (acknowledging societal expectation prior to digital age); *Jones*, 565 U.S. at 430 (outlining society's expectations regarding surveillance of individual's movements); United States v. Hammond, 996 F.3d 374, 388 (7th Cir. 2021) (acknowledging Supreme Court's prior reasoning regarding long-term individual surveillance).

146. *See Carpenter*, 138 S. Ct. at 2219-20 (analyzing third-party doctrine in context of novel CSLI); Lux, *supra* note 8, at 115 (arguing straightforward application of *Carpenter* to tower dump CSLI).

147. *See Carpenter*, 138 S. Ct. at 2219 (acknowledging "world of difference" between CSLI and pen register in *Smith*); Smith v. Maryland, 442 U.S. 735, 741-42 (1979) (analyzing pen registers' limited capability in only establishing phone numbers dialed); Lux, *supra* note 8, at 116 (arguing CSLI implicates greater privacy concerns than pen registers).

148. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (noting CSLI not shared voluntarily in any meaningful sense); Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner, *supra* note 3, at 4 (arguing CSLI created involuntarily, without conscious thought); Kortz & Bavitz, *supra* note 2, at 28-29 (suggesting *Carpenter*'s holding on third-party doctrine straightforward application to tower dumps); Lux, *supra* note 8, at 115 (extending reasoning in *Carpenter* to tower dumps).

149. *See Carpenter*, 138 S. Ct. at 2220; Lux, *supra* note 8, at 115 (arguing third-party doctrine not applicable to tower dump CSLI).

B. A Traditional Tower Dump Warrant Is Analogous to an All-Person Warrant

A tower dump warrant is analogous to an all-person warrant that the Supreme Court and lower courts have prohibited.[150] In *Ybarra v. Illinois*, law enforcement executed an all-person search warrant that authorized the search of a tavern, and proceeded to search all persons on the premises.[151] In *Commonwealth v. Perry*, law enforcement obtained a tower dump warrant that authorized the disclosure of CSLI and PII for all users present at or near the crime scene during its occurrence.[152] With no constraint in the warrant, law enforcement were free to request CSLI and PII—thus conducting a search—of any and all users they wanted.[153] In both scenarios, the warrant specified a place to be searched but provided no restriction as to who may be searched; this allowed law enforcement to search anyone present at the time they executed the search .[154]

1. A Lack of Probable Cause for All Users

Tower dump warrants requesting CSLI and PII for all users cannot meet the probable cause requirement because probable cause does not exist for all the users included in the tower dump; in fact, most users are completely innocent and unconnected to the alleged crime.[155] Courts that have addressed the argument of lack of probable cause for a tower dump have stopped their analysis too early by only focusing on whether law enforcement had probable cause to search the suspect.[156] An all-person warrant requires there to be probable cause particularized to *each* person to be searched; therefore, a tower dump warrant requesting CSLI

150. *See, e.g.*, Ybarra v. Illinois, 444 U.S. 85, 90-91 (1979) (rejecting search of all persons present at location specified in warrant); Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004) (approving all-person warrants only when probable cause attaches to each person); Marks v. Clarke, 102 F.3d 1012, 1025 (9th Cir. 1996) (articulating law clearly prohibits warrants for all persons present somewhere). *Compare Ybarra*, 444 U.S. at 88 (outlining all-person warrant and subsequent search of all persons), *with Perry II*, 184 N.E.3d 745, 768-69 (Mass. 2022) (discussing how tower dump warrant authorized search of all users present within designated location).

151. *See Ybarra*, 444 U.S. at 88 (outlining scope of search warrant issued).

152. *See Perry II*, 184 N.E.3d at 768-69 (discussing tower dump warrant's scope).

153. *See id.* at 769 (reasoning warrant impermissibly broad on its face). The Massachusetts SJC reasoned the accompanying affidavit, which specified law enforcement sought to identify a common phone number, made the warrant sufficiently particular. *See id.*

154. *Compare Ybarra*, 444 U.S. at 88, *with Perry II*, 184 N.E.3d at 768-69.

155. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (noting thousands of users searched in tower dump); Owsley, *supra* note 6, at 18 (outlining large numbers of users potentially caught in tower dumps).

156. *See* Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004) (requiring probable cause of criminal activity for all persons present at time of search); *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 751 (N.D. Ill. 2020) (asserting probable cause analysis applied only to defendant stops short of full inquiry). In analyzing the probable cause requirement for a geofence warrant, one court found a tower dump analysis unpersuasive because it did not extend to whether probable cause existed for uninvolved users. *See In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751 (declining to follow cited case).

and, or PII should require probable cause particularized to *each* phone number identified.[157]

Yet, a user can be nowhere near the crime scene but still implicated in a tower dump—and therefore searched—because CSLI may only place the user's location down to a few hundred feet.[158] Tower dumps are also executed in public areas that would clearly implicate users who are unconnected to the criminal activity.[159] In one investigation, law enforcement requested numerous tower dumps covering public areas surrounding convenience stores; collectively, the tower dumps yielded over 50,000 unique phone numbers.[160] While probable cause is a fluid concept, law enforcement cannot simply justify a tower dump warrant by pointing to the fact that innocent users were in close proximity to a suspect.[161] Similarly, police cannot merely rely on the fact they have probable cause for the crime scene to search every cell phone user who comes near.[162] A court, therefore, cannot find probable cause with respect to all users implicated in a tower dump warrant because law enforcement cannot demonstrate a sufficient probability innocent users will be connected to the criminal activity.[163]

157. *See* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (requiring particularized probable cause to search each person); Marks v. Clarke, 102 F.3d 1012, 1029 (9th Cir. 1996) (explaining all-person warrant appropriate only when reason to believe each person connected to criminal activity); *Owens*, 372 F.3d at 276 (affirming narrow circumstances when all-person warrant constitutional); *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751 (asserting probable cause analysis also extends to innocent users). It is impossible to require particularized probable cause for each phone number in a tower dump because law enforcement has no way of knowing which users will be ensnared. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (acknowledging law enforcement does not have to identify suspected users prior to tower dump request).

158. *See* Hoover, *supra* note 22, at 745 (suggesting accuracy of GPS greater than CSLI); Kortz & Bavitz, *supra* note 2, at 27 (explaining CSLI precision varies from few miles to single city block or greater); Owsley, *supra* note 6, at 33 (suggesting CSLI accuracy greatly varies but increasing). A couple hundred feet is a large enough area to ensnare many innocent users and subject them to a search. *See* LEVINSON-WALDMAN, *supra* note 3, at 2 (asserting thousands of users caught in tower dump); Owsley, *supra* note 6, at 18 (suggesting large numbers of users risk potential search in tower dumps). Advanced cell sites, however, could place users down to the floor of a building in some areas. *See Perry II*, 184 N.E.3d 745, 753 (Mass. 2022).

159. *See* United States v. Walker, No. 18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *5 (E.D.N.C. July 20, 2020) (outlining warrant for search of public locations over several hours); State v. Hudson, No. 1809009750, 2021 Del. Super. LEXIS 670, at *3-4 (Del. Super. Ct. Nov. 23, 2021) (discussing use of tower dump closest to public bank); *Perry II*, 184 N.E.3d at 755 (stating over 50,000 phone numbers obtained in tower dumps in public areas); LEVINSON-WALDMAN, *supra* note 3, at 2 (noting use of tower dump near several banks, netting over 100,000 phone numbers).

160. *Perry II*, 184 N.E.3d at 754-55 (discussing factual circumstances of case).

161. *See* Illinois v. Gates, 462 U.S. 213, 232 (1983) (affirming fluidity of probable cause turning on probabilities under specific factual circumstances); *Ybarra*, 444 U.S. at 91 (asserting proximity to another suspect insufficient to establish particularized probable cause).

162. *See Ybarra*, 444 U.S. at 91 (emphasizing probable cause requirement).

163. *See supra* notes 158-159, 161-162 and accompanying text (reasoning lack of probable cause for all persons potentially implicated in CSLI search).

2. A Lack of Particularity

A tower dump warrant that does not restrict law enforcement's ability to obtain CSLI and PII cannot meet the particularity requirement.[164] The Supreme Court has described the particularity requirement as strict, requiring the warrant to leave no discretion for law enforcement executing it.[165] But in a typical tower dump warrant requesting to search CSLI of users who fall within the search parameters, law enforcement may search any and all users at their discretion in violation of the particularity requirement.[166] Additionally, law enforcement lacks the necessary particularized probable cause for every user that ends up ensnared in the report.[167]

Courts that have found a tower dump warrant to be constitutional have reasoned the time constraint satisfies the particularity requirement.[168] But this rationale ignores the fact that an all-person search warrant is similarly constrained to a limited time period: the time it takes law enforcement to physically execute the search.[169] This basis of support for a tower dump warrant is unpersuasive

164. *See supra* note 78 (discussing particularized probable cause for each person searched required to satisfy requirement); *Perry II*, 184 N.E.3d 745, 768-69 (Mass. 2022) (explaining lack of constraint would constitute general warrant in violation of particularity).

165. *See* Marron v. United States, 275 U.S. 192, 196 (1927) (suggesting law enforcement allowed no discretion in executing warrant); Stanford v. Texas, 379 U.S. 476, 485 (1965) (affirming general searches impossible due to constitutional requirement of particularity).

166. *See Marron*, 275 U.S. at 196 (insinuating no discretion permitted for law enforcement when conducting search); United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982) (requiring specificity in warrant permitted by circumstances); *James I*, No. 18-cr-216 (SRN/HB), 2018 U.S. Dist. LEXIS 210433, at *3 (D. Minn. Nov. 26, 2018) (identifying no constraint in officer's investigation of cellular information); *Perry II*, 184 N.E.3d at 768-69 (noting law enforcement could pick any phone number to search without even iota of suspicion). In one Massachusetts case, the SJC acknowledged this warrant would allow law enforcement to obtain CSLI and search users without limitation or "even an iota of suspicion." *See Perry II*, 184 N.E.3d at 769 (addressing Perry's argument tower dump warrant not sufficiently particular). The SJC, however, noted the deficiency in the warrant was remedied by the supporting affidavit, which explained that law enforcement was seeking to identify a common phone number between tower dumps. *See id.* (determining scope of search limited by affidavit).

167. *See supra* notes 158-159, 161-162 and accompanying text (reasoning particularized probable cause does not exist for all users in tower dump reports).

168. *See James II*, 3 F.4th at 1106 (8th Cir. 2021) (reasoning temporal constraint meets particularity); State v. Hudson, No. 1809009750, 2021 Del. Super. LEXIS 670, at *24 (Del. Super. Ct. Nov. 3, 2021) (expressing time constraint satisfies particularity requirement). Tower dump warrants are constrained in that they explicitly provide a relatively limited timeframe to search, spanning between minutes and hours. *See Perry I*, No. 146144, 1984CR00396, 2021 Mass. Super. LEXIS 49, at *2-3 (Mass. Super. Ct. Apr. 21, 2021) (noting timeframes of fifteen to forty minutes before and after crime specified); United States v. Walker, No. 18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *5 (E.D.N.C. July 20, 2020) (outlining warrant description for five hours of CSLI); *Hudson*, 2021 Del. Super. LEXIS 670, at *3-4 (explaining over seven hours of CSLI sought in warrant). Yet, law enforcement can also request multiple tower dumps that span across several days. *See Perry II*, 184 N.E.3d at 754 (noting first search warrant requested tower dumps across four days).

169. *See* Ybarra v. Illinois 444 U.S. 85, 88-89 (1979) (explaining law enforcement's execution of search warrant); Owens v. Lott, 372 F.3d 267, 271-72 (4th Cir. 2004) (describing law enforcement's limited search at time of execution).

because both warrants specify only a location and the timeframe of the search in either case is constrained.[170]

C. Complying with the Warrant Requirements

1. Complying with Probable Cause

In order to satisfy the probable cause requirement, law enforcement should be restricted to only obtaining CSLI and PII for common phone numbers.[171] Law enforcement should only be permitted to request phone numbers in their original tower dump request because they do not have probable cause to search all users and therefore cannot request CSLI and PII for all users.[172] Rather, after law enforcement has obtained numerous tower dump reports, they law enforcement can cross reference the phone numbers to identify any common numbers present across numerous prior tower dump reports.[173] If a common phone number is identified, law enforcement then may have probable cause to search that user and therefore may request that user's CSLI or PII.[174]

2. Complying with Particularity

To comply with the particularity requirement in particularly describing who is to be searched, the use of a tower dump should be restricted to investigations where multiple tower dumps can be used to identify a common phone number of interest.[175] The privacy concerns inherent in a tower dump generally outweigh the perceived benefit in requesting a single tower dump because it is nearly impossible for law enforcement to narrow down all the phone numbers and identify a suspect.[176] With multiple tower dump reports, law enforcement can specify in the warrant they are seeking to search—and obtain CSLI and PII for—those

170. *Compare Ybarra*, 444 U.S. at 88 (constraining search to specified location and time of execution), *with supra* note 168 (noting time and location constraints in warrant based on crime).

171. *See infra* note 174 (supporting probable cause requirement before CSLI of user can be requested).

172. *See supra* notes 161-162 and accompanying text (explaining probable cause does not exist for innocent cell phone users caught in tower dump).

173. *See supra* note 53 (outlining cases where law enforcement cross-referenced phone numbers across tower dumps to successfully identify suspect).

174. *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) (affirming probable cause requires only fair probability of criminal evidence); *Perry I*, No. 1984CR00396, 2021 Mass. Super. LEXIS 49, at *8 (Mass. Super. Ct. Apr. 21, 2021) (determining probable cause existed for common phone numbers).

175. *See* U.S. CONST. amend. IV (requiring express *particular* description); *Perry I*, 2021 Mass. Super. LEXIS 49, at *8 (authorizing warrant in part because investigation involved serial crime); LAFAVE, *supra* note 79, § 4.5(e) at 2 (discussing issue in warrant seeking to search persons present).

176. *See supra* notes 52-54 and accompanying text (describing tower dump's particular usefulness for serial crimes). Given the broad reach of tower dumps, it is unclear whether a tower dump could ever only ensnare the specific user law enforcement happen to be looking for. *See supra* note 51 and accompanying text (highlighting high number of users ensnared in tower dumps).

phone numbers present across numerous reports.[177] Requiring law enforcement to specify that they are seeking a common phone number would distinguish a tower dump warrant from an all-person warrant because it would constrain *who* law enforcement could search to only those common phone numbers.[178] This constraint should be no additional burden, as law enforcement already cross references phone numbers across tower dump reports to identify those present at numerous crime scenes.[179]

IV. CONCLUSION

Tower dump CSLI can be deeply revealing, and the privacy intrusion only increases when it can be linked to a named user. Cell phones continuously generate CSLI and allow providers to compile an infallible, precise, and detailed record of the user's movements. These records are created for every cell phone user and access greatly expands the government's surveillance capabilities by providing otherwise unknowable information about any user. As traditional tower dump warrants are analogous to unconstitutional all-person warrants, law enforcement should be required to obtain probable cause before requesting a user's CSLI or PII. Constraining CSLI and PII requests to common phone numbers allows a tower dump warrant to comply with the warrant requirements by providing probable cause and particularly by naming who will be searched. Such constraints simultaneously help to preserve the degree of privacy that advancing technology seeks to erode for all cell phone users.

177. *See Perry I*, 2021 Mass. Super. LEXIS 49, at *4 (suggesting tower dump authorized partly because serial crimes at issue); *supra* note 53 (outlining cases where law enforcement cross reference phone numbers across tower dumps to identify suspect).

178. *See* Ybarra v. Illinois 444 U.S. 85, 91 (1979) (clarifying probable cause standard requires particularized probable cause for each individual); Marks v. Clarke, 102 F.3d 1012, 1019 (9th Cir. 1996) (asserting warrant authorized search of all persons on premises of search).

179. *See supra* note 53 (listing cases where tower dump warrants used for serial crimes to single out one number).