# CELL SITE LOCATION INFORMATION: A CATALYST FOR CHANGE IN FOURTH AMENDMENT JURISPRUDENCE

*By V. Alexander Monteith*[*]

## I. INTRODUCTION

As technology evolves, courts struggle to address Fourth Amendment issues related to the advancement of technology while balancing the privacy of citizens and the needs of the government. On one hand, advances in technology assist law enforcement investigations, on the other, these advancements inevitably provide new avenues for the government to infringe upon personal privacy.[1] With the advancement of technology and the widespread use of smartphones, government use of cell site location information (CSLI) without a warrant has become a controversial topic.[2] The Stored Communications Act (SCA) permits government officials and members of law enforcement agencies to collect CSLI from mobile phone providers.[3] The government obtains CSLI through cellular towers that constantly communicate with mobile phones and provide law enforcement with subscriber location data that would otherwise be private information.[4] Under the SCA, law enforcement can obtain CSLI from cell service providers (CSPs) without a search warrant, meeting the standard for

[*] J.D. Candidate 2018, University of Kansas School of Law; B.A. 2014 (History), University of South Florida. I would like to thank the members of my family for their love and support during the writing process, specifically, my mother Re Monteith, father Lt. Col. Alex Monteith, brother David Monteith, girlfriend Natalie Emerson, grandmother Teri Monteith, and aunts Dr. Jennifer Monteith and Lt. Col. Laura Monteith. Additionally, I appreciated the insight and guidance of my faculty advisor, Elizabeth Cateforis, and the members of the *Kansas Journal of Law & Public Policy* for their editing efforts.

1. *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012) (considering Fourth Amendment context of warrantless GPS technology); Kyllo v. United States, 533 U.S. 27 (2001) (considering Fourth Amendment context of thermal imaging devices on a residence); United States v. Karo, 468 U.S. 705 (1984) (considering Fourth Amendment context of beeper technology).

2. Elizabeth Gula Hodgson, Comment, *The Propriety of Probable Cause: Why the U.S. Supreme Court Should Protect Historical Cell Site Data with a Higher Standard*, 120 PENN. ST. L. REV. 251, 255–56 (2015).

3. *See* 18 U.S.C. § 2703 (2012).

4. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007) (describing the process in which cell phones relay location information to cell towers in a process known as "registration").

reasonable suspicion and using a court order as a substitute, which does not bear the same burden of proof of probable cause as a warrant.[5] The advances in CSLI technology, combined with the SCA and the judicially created third-party doctrine, have created a need for Fourth Amendment jurisprudence reform.[6]

This article addresses government use of warrantless CSLI, the public policy concerns inevitably entangled with the government use of CSLI, and the modern implications of the Fourth Amendment's third-party doctrine. Part II of this article explains the technology behind CSLI. Part III provides background information regarding the Fourth Amendment of the United States Constitution as it pertains to CSLI and the SCA. Part IV discusses current trends in case law and the rationales used by courts when ruling in cases dealing with CSLI. Part V investigates the separate policy concerns with CSLI technology involving the public, the government, and CSPs. Part VI analyzes a cell phone user's Fourth Amendment protection in CSLI in light of *Katz* and the third-party doctrine. Part VII condemns warrantless government search of CSLI, provides potential remedies for warrantless government searches in light of policy concerns, and argues that the third-party doctrine in Fourth Amendment jurisprudence is out of touch with the technological era and must be reconsidered.

## II. CSLI TECHNOLOGY BACKGROUND

The overwhelming majority of Americans own cell phones. By 2015, ninety-two percent of Americans owned a mobile phone and sixty-four percent of Americans owned a smartphone.[7] Based on the U.S. population of 324,000,000 people, this amounts to 291,600,000 Americans with a mobile phone.[8] As cell phones pervade modern society, our lives become more convenient; however, our personal lives have never been subject to such surveillance and people are beginning to resist the gradual invasions of personal privacy.[9] The ability to collect more precise location data has advanced to the point that it now rivals the precision and accuracy of global positioning systems (GPS) because the number of cellular towers has increased to keep up with the number of cellular phones.[10] Over time, CSLI technology has continued to

5. *See* 18 U.S.C. § 2703(c)(1)(B) (2012).

6. Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 680 (2015) (stating that the third-party doctrine is "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties").

7. AARON SMITH, PEW RES. CTR., U.S. SMARTPHONE USE IN 2015 2 (2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

8. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, http://www.census.gov/popclock/ (last visited Oct. 6, 2016).

9. *See* Adrienne LaFrance, *The Convenience-Surveillance Tradeoff*, ATLANTIC (Jan. 14, 2016), http://theatlantic.com/technology/archive/2016/01/the-convenience-surveillance-tradeoff/423891/.

10. *See Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary*, 113th Cong. 50, 53 (2013) [hereinafter *ECPA Part II*].

advance, providing increasingly detailed information about mobile phone users and their geographic whereabouts.[11]

Cell phones transmit and receive data through radio waves.[12] CSPs obtain CSLI through a mobile phone's constant communication with nearby cellular towers.[13] Whenever a cell phone user sends or receives any data–such as a text message, email, or phone call–the phone transmits data to the closest cellular tower using radio waves, thus producing CSLI.[14] Data is constantly transmitted, often without the user's knowledge; mobile phone users commonly install applications configured to constantly refresh and transmit data, even when unused.[15] Moreover, unless a cell phone is powered down or in airplane mode, the phone is constantly "pinging" the nearest tower, transmitting data, despite user inactivity.[16] On average, an inactive phone will "ping" to a tower every seven to nine minutes.[17] If a cell phone user's signal is lost due to distance from the tower, the phone will automatically connect to a closer tower without notifying the user.[18] In an urban environment, the closest cellular tower is typically only a few city blocks away.[19]

CSLI resulting from cell phone communication with towers reveals precise detail of a person's geographic location to cell service providers (CSPs).[20] CSPs can triangulate a phone user's location "based on the strength, angle, and timing of that cell phone's signal measured across multiple cell site locations."[21] CSPs set up towers and antennas in "sectors" which allows them to accurately pinpoint a user's location.[22] Using these techniques, CSPs can give the government detailed location data without the phone user's knowledge or voluntary consent; this can be as detailed as what floor the user is on in a specific building.[23] Modern technology allows for CSLI to be both historical and active, showing past and current locations of a cell phone user.[24] The government is responsible

---

11. *In re* Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1015 (N.D. Cal. 2015).

12. *ECPA Part II*, *supra* note 10, at 50.

13. Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Data Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1747 (2009).

14. *Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d at 1014.

15. *See, e.g.*, John Caniglia & Teresa Dixon Murray, *Amazon, Amazon-Related Apps Blamed for Some Verizon Data Overages*, CLEVELAND.COM (Sept. 29, 2016, 8:30 AM), http://cleveland.com/business/index.ssf/2016/09/amazon_amazon-related_apps_bla.html.

16. U.S. DEP'T OF HOMELAND SEC., LESSON PLAN: HOW CELL PHONES WORK 7, 9 (2010), https://www.eff.org/files/filenode/how_cell_phones_work.pdf.

17. *Id.* at 9.

18. *Id.*

19. *Id.* at 5.

20. *See* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1434 (2007).

21. *See In re* Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1015 (N.D. Cal. 2015); *ECPA Part II*, *supra* note 10, at 56.

22. *ECPA Part II*, *supra* note 10, at 53.

23. *See id.* at 52, 56.

24. *See* Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications*

for an alarming number of requests for CSLI; for example, AT&T reported that the government filed 64,703 requests in 2014.[25]

## III. FOURTH AMENDMENT AND STATUTORY BACKGROUND

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[26]

The Fourth Amendment's purpose is to protect the people's right to privacy from arbitrary governmental intrusions in the form of unreasonable searches and seizures.[27] The government conducts a search when (1) it infringes on a person's subjective expectation of privacy and (2) society recognizes that expectation as reasonable.[28] The Supreme Court has long held that a warrantless search is *per se* unreasonable and constitutes a Fourth Amendment violation, subject to a few well-delineated exceptions, such as an exigent circumstance.[29] Courts consider cell phones "effects" under the Fourth Amendment's "persons, houses, papers, and effects" clause, qualifying them for Fourth Amendment protection from unreasonable searches and seizures.[30]

In a series of cases in the 1970s, the Supreme Court judicially created the third-party doctrine, which provides limits to Fourth Amendment protection.[31] The third-party doctrine states, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[32] In *Miller*, the Court held that the government's warrantless search of defendant's bank records did not violate the Fourth Amendment because Miller had no expectation of privacy in the bank's business records once he had entrusted the information to the bank.[33] Subsequently, in *Smith*, government use of a pen

---

*Act: Why the Warrantless Gathering of Historical Cell Site Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 710 (2012).

25. Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, ATLANTIC (Aug. 8, 2016), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/.

26. U.S. CONST. amend. IV.

27. *See* Legal Information Institute, *Fourth Amendment: An Overview*, CORNELL U. L. SCH., https://www.law.cornell.edu/wex/fourth_amendment (last visited Oct. 17, 2016).

28. United States v. Leon, 468 U.S. 897, 931 (1984).

29. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

30. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

31. *See* Smith v. Maryland, 442 U.S. 735, 735 (1979); *see also* United States v. Miller, 425 U.S. 435, 435 (1976).

32. *Smith*, 442 U.S. at 743–44.

33. *Miller*, 425 U.S. at 446.

register to collect phone numbers dialed on defendant's home phone did not violate the Fourth Amendment because defendant voluntarily conveyed that information when he dialed the number and the pen register did not reveal the content of the call.[34] The Court reasoned that the defendant's monthly phone bill provided notice that the information was being collected because it listed all of the numbers defendant dialed.[35] Thus, under the third-party doctrine, none of the information voluntarily given to a third-party, such as CSPs, receives any protection under the Fourth Amendment because it fails the two-part test set out in *Katz v. United States*.[36]

*Katz* ushered in a new era of Fourth Amendment jurisprudence and forever changed what courts consider a search.[37] The Supreme Court held that the Fourth Amendment protects "people not places."[38] The *Katz* court created a two-part test that has become essential in analyzing Fourth Amendment issues and determining whether a person's expectation of privacy is reasonable.[39] In step one of the *Katz* test, a court must determine whether a person has a subjective expectation of privacy; courts look to whether a person took actions that show a desire to keep information private.[40] In step two of the *Katz* test, a court must determine whether there is an objective expectation of privacy; courts ask whether society as a whole recognizes the privacy interest as reasonable.[41]

Information voluntarily given to third-parties fails the second part of the *Katz* test. This is because society does not recognize a reasonable privacy interest in information disclosed to third-parties.[42] Therefore, information voluntarily conveyed to third-parties is not subject to Fourth Amendment protection and may be searched without a warrant.[43]

In reaction to the Supreme Court's creation of the third-party doctrine in the 1970s,[44] Congress enacted Title II of the Electronic Communications Privacy

---

34. *See id.* at 742.

35. *Id.*

36. *See Smith*, 442 U.S. at 743–44 (holding that it is unreasonable to have a subjective expectation that the phone numbers dialed would remain private); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (holding that for a privacy interest to be recognized, society must deem the interest to be reasonable).

37. *See* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) ("When that self-indulgent [*Katz*] test is employed . . . to determine whether a 'search or seizure' within the meaning of the Constitution has occurred . . . it has no plausible foundation in the text of the Fourth Amendment.").

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

39. *Id.* at 361 (Harlan, J., concurring); *see, e.g.*, California v. Ciraolo, 476 U.S. 207, 218 (1986) (stating *Katz* was a "landmark decision").

40. *Katz*, 389 U.S. at 351, 361.

41. *Id.* at 353.

42. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

43. *Id.* at 743–44.

44. *See, e.g., Smith*, 442 U.S. at 735 (holding that government use of a pen register is not an unreasonable search under the Fourth Amendment); United States v. Miller, 425 U.S. 435, 435 (1976) (holding that defendant had no right to Fourth Amendment protection because his bank records were voluntarily conveyed to a third party and were part of the bank's business records).

Act (ECPA).[45] Within the ECPA, the SCA "set forth the circumstances under which a 'government entity' may 'require' disclosure of electronic information from service providers."[46] Subsection (c) addresses the standard for CSP disclosure of CSLI:

> (c) Records concerning electronic communication service or remote computing service.
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
> (B) obtains a court order for such disclosure under subsection (d) of this section.[47]

Congress enacted this legislation to provide protection for people's private electronic communications stored by service providers.[48]

As society has become more digitized, the advancement of technology has challenged the SCA's effectiveness in protecting American citizens.[49] For example, in *United States v. Jones*, the Court supplemented the *Katz* test while holding that warrantless tracking using a GPS tracking device was an unreasonable search that violated the Fourth Amendment.[50] The Court supported its decision using the theory of common law trespass, adding the trespass analysis in addition to the two-part privacy test used in *Katz*.[51]

In *Jones*, law enforcement officials attached a GPS tracking device to the defendant's vehicle without a warrant and monitored Jones's movement for twenty-eight days in connection with a narcotics investigation.[52] The government used the collected data to secure an indictment, charging Jones as well as several co-conspirators on conspiracy to traffic narcotics.[53] The Court held that this violated the Fourth Amendment because it constituted a trespass.[54] The Court did not address whether the GPS tracking violated the *Katz* test,

45. *See* Electronic Communication Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522 (1986)).

46. Claudia G. Catalano, Annotation, *Criminal Defendant's Rights Under Stored Communications Act, 18 U.S.C.A. § 2701 et seq.*, 11 A.L.R. Fed. 3d Art. 1 (2016).

47. 18 U.S.C. § 2703(c)(1) (2012).

48. *See* Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 40 (2015).

49. *See* Robert A. Pikowsky, *The Need for Revisions of the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 2 (2003).

50. *See* United States v. Jones, 565 U.S. 400, 404, 413 (2012).

51. *See id.* at 400.

52. *See id.* at 403.

53. *See id.* at 403.

54. *See id.* at 410.

leaving unanswered the question of whether people have an expectation of privacy in their geographic location.[55] Instead, the Court suggested that it is possible that warrantless long-term monitoring of a person's location and movements would violate the Fourth Amendment.[56] The decision and approach of analysis in *Jones* was a significant shift from *Katz,* reemphasizing the Fourth Amendment protection of places as well as people.[57]

In Justice Sotomayor's concurring opinion, she suggested that it might be time to change the third-party doctrine.[58] She cited the advancement of technology as a catalyst for change by stating that the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[59] Similar to CSLI, Justice Sotomayor noted how GPS tracking allows the government and individuals to take the aggregate of information obtained and make reasonable inferences about an individual's private life.[60] In this respect, CSLI is comparable to GPS because it allows government aggregation of personal data. Additionally, she suggested that society might recognize an interest in keeping the sum of one's movements private.[61]

In *Jones*, the Court metaphorically kicked the can down the road; it failed to adequately address the third-party doctrine and society's recognition of privacy interests in geographic locations.[62] Moving forward, it will be intriguing to see how the Court will approach Fourth Amendment questions, because the trespass theory will probably not be practicable to justify a ruling involving CSLI since there is no physical intrusion when the government obtains CSLI. The future resolution of Fourth Amendment cases is uncertain, especially in light of the passing of Justice Scalia, the author of the *Jones* opinion and a key proponent of the "trespass" theory in Fourth Amendment cases.[63]

While Congress implemented the SCA to provide greater protection for the American people, lawmakers in the 1980s likely could not have predicted the sheer volume of digital data electronically transmitted or how private information is now shared.[64] Under § 2703(c)(1) of the SCA, the government can obtain CSLI information from CSPs through a search warrant or a court

55. *See id.* at 412–13.
56. *See id.* at 413.
57. *See id.* at 406–07.
58. *See id.* at 417 (Sotomayor, J., concurring).
59. *Id.*
60. *See id.* at 415.
61. *See id.* at 416.
62. *See id.* at 412 (majority opinion).
63. Adam Liptak, *Antonin Scalia, Justice on the Supreme Court, Dies at 79*, N.Y. TIMES (Feb. 13, 2016), http://www.nytimes.com/2016/02/14/us/antonin-scalia-death.html?_r=0; Jonathan Banks, *Justice Scalia: Underappreciated Fourth Amendment Defender*, CATO INST. (Feb. 15, 2016), https://www.cato.org/blog/justice-scalia-underappreciated-fourth-amendment-defender.
64. *See* Max Bauer, *Will Congress Mandate a Warrant for Access to Our Emails? What About Location Tracking?*, PRIVACYSOS (Apr. 12, 2013), https://privacysos.org/blog/will-congress-mandate-a-warrant-for-access-to-our-emails-what-about-location-tracking/.

order.[65] While the two methods might seem similar, each method requires a different burden of proof.[66]

For a law enforcement officer to obtain a search warrant, he or she must sign an oath or affirmation attesting to the foundation of the evidence and the need to conduct a search.[67] A neutral magistrate must approve that there is "probable cause," and the warrant must specifically state when, where, and what is sought to be searched.[68] The standard of "probable cause" does not demand absolute certainty, but rather a fair probability based on the totality of the circumstances.[69]

The burden of proof to obtain a court order under the SCA is less stringent than the "probable cause" standard necessary for a search warrant.[70] In order for the government to receive a court order, it must offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[71] This lower standard is comparable to the "reasonable suspicion" burden of proof in criminal law, which requires significantly less proof than probable cause.[72]

Because the government is not required to show probable cause under the less stringent standard, many question whether this constitutes an unreasonable search under the Fourth amendment.[73] The Court has not had the occasion to decide whether the court order provision violates the Fourth Amendment. Arguably, such a search without a warrant may violate the *Katz* test.[74] Courts have analyzed this complex issue in different ways.

## IV. ANALYSIS AND TRENDS OF CSLI CASES

Since 2010, several CSLI cases have been litigated in lower Federal Courts and State Supreme Courts.[75] These courts have analyzed Fourth Amendment

65. 18 U.S.C. § 2703(c)(1)(A)–(B) (2012).

66. *See In re* Application of the U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010).

67. *See* Legal Information Institute, *Search Warrants: An Overview*, CORNELL U. L. SCH., https://www.law.cornell.edu/wex/search_warrant (last visited Oct. 17, 2016).

68. *Id.*

69. *See* Illinois v. Gates, 462 U.S. 213, 246 (1983).

70. *See, e.g.*, United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015) (en banc); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013); *In re Application of the U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 315.

71. 18 U.S.C § 2703(d) (2012).

72. *See* Terry v. Ohio, 392 U.S. 1, 37 (1968) (explaining the probable cause standard required to obtain a warrant is a higher burden of proof than reasonable suspicion).

73. *See In re Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 313–18.

74. *See* McLaughlin, *supra* note 4, at 444–45.

75. *See, e.g.*, United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir.

jurisprudence differently and have produced vastly different results.[76] The Court's reluctance to reevaluate the third-party doctrine has been the key factor in the disparity of the outcomes in Federal and State courts in deciding CSLI cases.

### *A. Federal Court Decisions*

Recent trends suggest that federal courts want to change the third-party doctrine to recognize a Fourth Amendment privacy right for CSLI, but are hesitant to contradict Supreme Court precedent.[77] All federal circuit courts who have heard CSLI cases held that obtaining CSLI via court order is not a Fourth Amendment violation.[78] A circuit split on the issue was remedied after the Eleventh and Fourth Circuits issued *en banc* judgments reversing their original findings that the government warrantless CSLI was not a violation of the Fourth Amendment.[79]

The disagreement between courts on whether obtaining warrantless CSLI is valid under the Fourth Amendment comes from disagreement on the application of the third party-doctrine. Most federal circuit courts have taken a similar stance to the United States District Court of Connecticut, which acknowledged the shortcomings of the third-party doctrine in the digital age stating "the third-party doctrine has been subject to tsunamis of criticism. But it doubtlessly remains good law today."[80] Because the Court has not created exceptions to the third-party doctrine, federal circuit court judges are bound to hold that warrantless government use of CSLI information does not violate the

---

2013); *In re* Application of the U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010); *In re* Application for Tel. Info. Needed for a Crim. Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); Tracey v. State, 152 So.3d 504 (Fla. 2014); Zanders v. State, 73 N.E.3d 178 (Ind. 2017); Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014); State v. Earls, 70 A.3d 630 (N.J. 2013).

76. *See, e.g., Carpenter*, 819 F.3d at 887 (holding that obtaining CSLI with a court order did not violate the Fourth Amendment); *Graham*, 824 F.3d at 450 (holding that CSLI can be obtained without a warrant via court order); *Davis*, 785 F.3d at 502 (same); *Historical Cell Site Data*, 724 F.3d at 615 (same); *Application of the U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 319 (same); *cf. Application for Tel. Info. Needed for a Crim. Investigation*, 119 F. Supp. 3d at 1012 (holding the CSLI cannot be obtained without a search warrant); *Tracey*, 152 So.3d at 526 (holding that obtaining historical and prospective CSLI without a search warrant violated the Fourth Amendment of the United States Constitution); *Augustine*, 4 N.E.3d at 858 (holding that under the Massachusetts State Constitution acquiring CSLI requires a search warrant); *Earls*, 70 A.3d at 643–44 (holding that under the New Jersey State Constitution acquiring CSLI requires a search warrant).

77. *See, e.g., Davis*, 785 F.3d at 498; *Graham*, 824 F.3d at 421; *Application for Tel. Info. Needed for a Crim. Investigation*, 119 F. Supp. 3d at 1011.

78. *See Carpenter*, 819 F.3d at 887; *Graham*, 824 F.3d at 450; *Davis*, 785 F.3d at 502; *Historical Cell Site Data*, 724 F.3d at 615; *Application of the U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 319.

79. *See Graham*, 824 F.3d at 450; *Davis*, 785 F.3d at 502.

80. United States v. Chavez, No. 3:14-cr-00185 (JAM), 2016 U.S. Dist. LEXIS 22312, at *5 (D. Conn. Feb. 24, 2016).

Fourth Amendment.[81] Along with *stare decisis* considerations, federal circuit courts have posited that a legislative remedy to the SCA is more appropriate than a judicially created one, stating a democratically elected body is in a better position to codify into law what society is willing to recognize as reasonable.[82]

The few federal courts that have ruled against warrantless government use of CSLI have justified their rulings by attacking the voluntariness requirement in the third-party doctrine.[83] These courts assert that cell phone users do not *voluntarily* convey their CSLI to CSPs.[84] The courts support this theory by acknowledging that no affirmative act by the user is necessary: "CSLI for a cellular telephone may still be generated in the absence of user interaction with a cellular telephone."[85] This idea has not won out in federal court – subsequent *en banc* hearings of these few cases reversed these decisions.[86]

### *B. State Supreme Court Decisions*

While the federal circuit courts show reluctance to hold that the warrantless use of CSLI violates individual privacy, state supreme courts are much more progressive. State supreme courts have held that warrantless government use of CSLI is unconstitutional based on both state constitutions and the United States Constitution; specifically, the Supreme Courts of Massachusetts and New Jersey based their rulings on their State Constitutions, while the Florida Supreme Court reached its ruling based on the Fourth Amendment in the United States Constitution.[87]

Both the Supreme Courts of Massachusetts and New Jersey dismissed the third-party doctrine and held that a person has a reasonable expectation of privacy in CSLI, noting that their State Constitutions provide greater protection than the Fourth Amendment in the United States Constitution.[88]

The majority of the Massachusetts court in *Augustine* completely rejected warrantless government use of CSLI and distinguished CSLI from data included in the third-party doctrine, stating that "the government here is not seeking to obtain information provided to the CSP by the defendant. Rather, it is looking only for the location-identifying by-product of the cellular telephone technology—a serendipitous (but welcome) gift to law enforcement investigations."[89] The court reasoned that times have changed since the third-

81. *See, e.g.*, *Davis*, 785 F.3d at 513.

82. *Carpenter*, 819 F.3d at 890.

83. *See, e.g.*, *Graham*, 796 F.3d at 356.

84. *See, e.g.*, *Graham*, 796 F.3d at 430–31; *Davis*, 785 F.3d at 1271; *Application for Tel. Info. Needed for a Crim. Investigation*, 199 F. Supp. 3d at 1027.

85. *Application for Tel. Info. Needed for a Crim. Investigation*, 199 F. Supp. 3d at 1027.

86. *See Graham*, 824 F.3d at 421; *Davis*, 785 F.3d at 498.

87. *See Tracey*, 152 So. 3d at 526 (Fla. 2014) (holding warrantless CSLI is a violation of the Fourth Amendment in the U.S. Constitution); *Augustine*, 4 N.E.3d at 858 (Mass. 2014) (holding warrantless CSLI is a violation of the Massachusetts State Constitution); *Earls*, 70 A.3d at 643–44 (N.J. 2013) (holding warrantless CSLI is a violation of the New Jersey State Constitution).

88. *See Augustine*, 4 N.E.3d at 858; *Earls*, 70 A.3d at 642.

89. *Augustine,* 4 N.E.3d at 863.

party doctrine's creation in the 1970s, stating cell phone use is essential to daily life, and that people need protection from privacy invasions.[90]

After considering the third-party doctrine, the New Jersey Supreme Court came to a different result, despite the fact that its analysis of the U.S. Constitution was strikingly similar to trends in Federal Courts.[91] The New Jersey Supreme Court in *Earls* held that individuals have a reasonable expectation of privacy in CSLI under the state constitution.[92] However, it also mentioned that, under the U.S. Supreme Court's holding in *Smith* and the third-party doctrine, the government is not required to obtain a warrant for CSLI under the Fourth Amendment of the U.S. Constitution.[93] Because both the decisions from Massachusetts and New Jersey were based on their state constitutions, they are not eligible for review by the U.S. Supreme Court.[94]

In contrast to the Supreme Courts of Massachusetts and New Jersey, the Florida Supreme Court held that warrantless real time and historical use of CSLI to track a defendant violated the Fourth Amendment to the U.S. Constitution.[95] The Florida Supreme Court heavily relied on Justice Sotomayor's concurring opinion in *Jones,* discussing the "mosaic" theory that suggests that government use of aggregate CSLI could allow the government to form reasonable inferences about a person's private life.[96] The court also discussed the third-party doctrine:

> Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes. While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction.[97]

The court acknowledged that people can prevent location information from being transmitted, but that powering off phones to prevent privacy invasions is an unreasonable burden on the public and does not prevent Fourth Amendment claims.[98] Last, the court asserted that phones are "effects" under the Fourth Amendment and are carried into protected areas, such as homes.[99] Thus, even with probable cause, obtaining CSLI without a warrant and while a defendant

90. *See id.* at 859.
91. *See Earls*, 70 A.3d at 644.
92. *Id.*
93. *Id.*
94. *See* Herb v. Pitcairn, 324 U.S. 117, 125–26 (1945) ("Our only power over state judgments is to correct them to the extent that they incorrectly adjudge federal rights.").
95. *See* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014).
96. *Id.* at 520.
97. *Id.* at 522.
98. *See id.* at 523.
99. *Id.* at 524.

was on a public road violated the Fourth Amendment.[100]

Similar to the federal courts, state supreme courts have issued conflicting rulings. Most recently, the Indiana Supreme Court ruled that warrantless government use of CSLI did not violate the Fourth Amendment, directly contradicting the Florida Supreme Court's decision.[101] Applying the third-party doctrine in *Smith* and *Miller*, the Indiana Supreme Court aligned with the current position of the federal circuit courts, seemingly not persuaded by other state supreme court rulings.[102]

Overall, recent trends in CSLI cases suggest that judges want to hold that warrantless CSLI is a Fourth Amendment violation, but are hesitant to stray from U.S. Supreme Court precedent. Despite being bound by precedent, courts acknowledge the shortcomings of the Fourth Amendment's third-party doctrine with respect to modern advances in technology.[103] In June 2017, the Court granted *certiorari* to hear *Carpenter v. United States*, and set oral arguments for October 2017.[104] Ideally, in *Carpenter*, the Court has the opportunity to address the third-party doctrine in Fourth Amendment jurisprudence and create new precedent to accommodate the vast changes in technology. Whether the Court takes advantage of this opportunity to modify the third-party doctrine or issues a narrow ruling only pertaining to CSLI remains to be determined.

## V. POLICY CONCERNS AND CSLI TECHNOLOGY

The heart of the Fourth Amendment is to effectively weigh the balance of public privacy against the needs of the state to protect citizens from danger.[105] While both public and government interests are important in society, courts have difficulty balancing these two competing forces to determine a search's "reasonableness" under a totality of the circumstances.[106] While determining a search's reasonableness under the Fourth Amendment, public policy interests of all parties involved must be analyzed to reach an equitable conclusion.

### *A. Policy Concerns of the Public*

As with most advances in technology, cell phones and government use of CSLI have many public benefits. As cell phones have become more versatile and comprehensive tools, they increasingly play an integral role in our daily

100. *See id.* at 525.

101. Zanders v. State, 73 N.E.3d 178, 189 (Ind. 2017).

102. *Id.* at 185.

103. *See e.g.*, United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) (en banc).

104. Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016), *cert. granted,* 137 S. Ct. 2211 (June 5, 2017). This case involves the government's use of warrantless CSLI to convict a defendant of aiding and abetting in a series of armed robberies at Radio Shack and T-Mobile stores in and around Detroit, Michigan. *Id.* at 884.

105. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

106. *See, e.g.*, Samson v. California, 547 U.S. 843, 848 (2006) ("[W]e 'examine the totality of the circumstances' to determine whether a search is reasonable within the meaning of the Fourth Amendment." (quoting United States v. Knights, 534 U.S. 112, 118 (2001))).

lives.[107] Collectively, Americans check their smartphones more than eight billion times a day.[108] The average American spends a total of five hours a day on their phone, or approximately one-third of their waking hours, which speaks to the importance of cell phones in our lives.[109]

CSLI allows for phone recovery. Losing a phone would be a significant inconvenience because cell phones contain essential information about our lives and serve as our primary mode of communication.[110] CSLI technology allows a person to trace their lost or stolen phone and accurately provides its real-time location, minimizing inconvenience, and allowing recovery of a phone that might not otherwise be recoverable.[111]

Additionally, CSLI has many beneficial applications for private sector employers. As technology has advanced, the number of employees working remotely or telecommuting has increased.[112] A growing number of employers allow employees to work remotely, providing flexibility and a more enjoyable work environment.[113] Telecommuting allows employers to retain employees that might have otherwise sought different employment opportunities due to geographic preference.[114] Having employees work outside of the traditional office space presents unique challenges; employers still retain an interest in preventing employee misconduct and ensuring employee efficiency.[115] CSLI technology provides employers with a means to monitor their employees during business hours on company owned phones.[116] For example, "a long-haul trucking company can keep track of their fleet of trucks and a taxicab company can determine where their drivers are at any time and in any location."[117]

---

107. *See* Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. TIMES (June 25, 2014), http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html.

108. *See* Lisa Eadicicco, *Americans Check Their Phones 8 Billion Times a Day*, TIME (Dec. 15, 2015), http://time.com/4147614/smartphone-usage-us-2015/.

109. *See* Carolyn Gregoire, *You Probably Use Your Smartphone Way More Than You Think*, HUFFINGTON POST (Nov. 2, 2015, 4:13 PM), http://www.huffingtonpost.com/ entry/smartphone-usage-estimates_us_5637687de4b063179912dc96.

110. *See* Michael McEnaney, *Lost Without Your Smartphone? Almost Half the Country Is, Too*, TECH TIMES (June 30, 2014, 9:17 PM), http://www.techtimes.com/articles /9449/20140630/lost-without-smartphone-half-country.htm (citing that 47% of the country says that they would feel lost without their cell phone for a single day).

111. *See* Bay City News Serv., *Tracking Software Leads Police to Stolen Cell Phone, Arrests*, MERCURY NEWS (Feb. 17, 2012, 3:52 PM), http://www.mercurynews.com /2012/02/17/tracking-software-leads-police-to-stolen-cellphone-arrests/.

112. *See* Jeffrey M. Jones, *In U.S., Telecommuting for Work Climbs to 37%*, GALLUP (Aug. 19, 2015), http://www.gallup.com/poll/184649/telecommuting-work-climbs.aspx (stating that telecommuting is up 7% over the past decade).

113. *See id.*

114. *See id.*

115. *See* Debbie Muller, *The HR Dilemma: Employee Misconduct or Just Work-Life Balance*, LINKEDIN (June 5, 2015), https://www.linkedin.com/pulse/hr-dilemma-employee-misconduct-just-work-life-balance-debbie-muller.

116. *See* Jen Manso, *Cell-Site Location Data and the Right to Privacy*, 27 SYRACUSE SCI. & TECH. L. REP 1, 2 (2012).

117. *Id.*

CSLI also has drawbacks that effect public privacy. CSLI technology's accuracy rivals GPS technology; in certain circumstances, it can even place an individual in a certain room or on a specific floor of a building.[118] The sum of an individual's location information can generate a "precise, comprehensive record of a person's public movements that reflects a wealth of detail about familial, political, professional, religious, and sexual associations."[119] Similar to GPS data, a person who obtains CSLI can access personal information which leaves "little to the imagination" to the purpose of a person's movements.[120] Even more alarming, the government can use algorithms to predict future movements and locations based on historical CSLI data.[121] An aggregate of CSLI can allow the reader of such data to establish patterns based on an individual's prior locations, allowing reasonable inferences to determine the nature of a person's visit. This leaves people vulnerable to the possible exposure of information they would otherwise reasonably expect to be private.

### *B. Policy Concerns of the Government and Law Enforcement*

When evaluating government use of CSLI under the Fourth Amendment, courts also look to the government interest to help determine the search's "reasonableness."[122] While CSLI technology presents many benefits to both the state and to law enforcement agencies, these benefits ultimately do not outweigh public privacy concerns in the context of warrantless government CSLI use.

CSLI technology can pinpoint the location of an emergency 911 call.[123] In situations that require a fast response from law enforcement, such as an active shooter, the median response time is approximately three minutes.[124] CSLI could help improve response times by providing an accurate location of the victims; this could lead to additional lives being saved.[125]

CSLI can help law enforcement apprehend suspects and fugitives at large.[126] For example, two robbery suspects were apprehended in California after police located them using a stolen cell phone equipped with Apple's cell

118. *See In re* Application for Tel. Info. Needed for a Crim. Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015).

119. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

120. *Id.*

121. *See* David Talbot, *A Phone That Knows Where You're Going,* MIT TECH. REV. (July 9, 2012), https://www.technologyreview.com/s/428441/a-phone-that-knows-where-youre-going/.

122. Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 992 (2004).

123. *See Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308 (2004); *Enhanced 911 - Wireless Services,* FCC, http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html (last visited Nov. 6, 2016).

124. *See* J. Pete Blair et al., *Active Shooter Events from 2000 to 2012*, FBI (Jan. 7, 2014), https://leb.fbi.gov/2014/january/active-shooter-events-from-2000-to-2012/view.

125. *See* Manso, *supra* note 116, at 2.

126. *See* Tracey v. State, 152 So. 3d 504, 507 (Fla. 2014) (stating that police used real time CSLI to locate defendant); State v. Earls, 70 A.3d 630, 633–34 (N.J. 2013) (stating how police used CSLI to track and locate a suspect at a motel).

phone tracker software.[127] Locating dangerous criminals efficiently and effectively benefits society by keeping the public safe and conserving law enforcement resources.

CSLI can also assist in locating missing individuals. For example, a Seattle man who was missing and threatening to commit suicide was found using CSLI and brought to a hospital to receive treatment before he could hurt himself.[128] In a missing persons case, time is of the essence; after fifty-one hours of a person going missing, the chances of survival are extremely low.[129] If a missing person has his or her cell phone and it is powered on, law enforcement could use CSLI to find them, providing a greater chance of survival.

One of CSLI technology's biggest potential benefits for the state and law enforcement is its ability to place a defendant at, or very close to, the scene of the crime. In *Commonwealth v. Augustine*, the state sought and received over sixty-four pages of CSLI information in order to "include or exclude" the defendant as a suspect in a murder investigation.[130] During a trial, the state may present CSLI information into evidence to prove the location of the defendant, further strengthening the credibility of their case.[131]

While CSLI has many positive applications for the government and law enforcement, there is potential for widespread abuse and misconduct. For example, a woman from Portland, Oregon was wrongly convicted of manslaughter and imprisoned for nearly a decade after law enforcement's warrantless use of CSLI.[132] The state's only evidence against her was CSLI that placed her at the scene of the crime. The prosecution used the weight of this evidence to influence the defendant to accept a guilty plea.[133] Almost a decade later, the woman was exonerated due to newly discovered DNA evidence.[134] In another example of warrantless government abuse of CSLI, a Minnesota woman petitioned for a restraining order against her former boyfriend, a member of a gang strike force.[135] The woman alleged that her boyfriend abused his power to access CSLI data to harass and stalk her.[136] The officer later resigned after a

127. Bay City News Serv., *supra* note 111.

128. Levi Pulkkinen, *Using Cell Phones to Find Missing Persons Pushes Law*, SEATTLEPI (May 4, 2008, 10:00 PM), http://www.seattlepi.com/local/article/Using-cell-phones-to-find-missing-persons-pushes-1272414.php.

129. Or. Health & Science Univ., *OHSU Researchers Find Time Is Best Predictor of Survival in Search and Rescue Missions*, OHSU (July 17, 2007), https://news.ohsu.edu/2007/07/17/ohsu-researchers-find-time-is-best-predictor-of-survival-in-search-and-rescue-missions.

130. Commonwealth v. Augustine, 4 N.E.3d 846, 850–51 (Mass. 2014).

131. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016) (stating that the prosecution used CSLI to place the defendant near the scene of a robbery).

132. *See* Douglas Starr, *What Your Cell Phone Can't Tell the Police*, NEW YORKER (June 26, 2014), http://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police.

133. *Id.*

134. *Id.*

135. Mara H. Gottfried, *Minneapolis Officer Quits amid Federal Probe of Metro Gang Strike Force*, PIONEER PRESS (Nov. 13, 2015, 6:48 PM), http://www.twincities.com/2009/08/28/minneapolis-officer-quits-amid-federal-probe-of-metro-gang-strike-force/.

136. *Id.*

federal investigation from the FBI into the alleged misconduct.[137]

CSLI is a powerful tool for law enforcement. Despite its many benefits, the potential for abuse and the invasion of privacy do not justify the warrantless use of CSLI of cell phone subscribers without meeting the standard of probable cause and obtaining a warrant.

### *C. Policy Concerns of Cell Service Providers (CSPs)*

Along with the concerns of the state and the public, the interests of CSPs and the effect of compelled CSLI disclosure on their business practices should also be considered. For many reasons, CSPs have a legitimate business interest in collecting CSLI from customers. Successful businesses strive to provide a quality experience to all customers. One-way CSPs can achieve this goal is by "optimizing cell and tower site coverage and availability."[138] Areas of high cellular traffic often hinder customers' service, and CSLI technology allows CSPs to determine high traffic areas based on usage, thus allowing companies to optimize their systems for maximum efficiency.[139]

Moreover, there is a lucrative industry for CSPs to collect cellular location data in particular, and sell this information to third parties seeking to target the public with advertisements or products.[140] All four major CSPs – Verizon, AT&T, Sprint, and T-Mobile – conduct this practice.[141] The fact that third-parties want CSLI to "target" individuals speaks to the wealth of information that can be derived and inferred from this information.

## VI. PRIVACY INTERESTS AND CSLI

The determination of whether warrantless government use of CSLI is a "search" under the Fourth Amendment starts with the two-part *Katz* test. The *Katz* test dictates that there must be a subjective expectation of privacy and an objective expectation of privacy that society is prepared to recognize as reasonable.[142]

### *A. Part One of the* Katz *Test: The Subjective Expectation of Privacy*

Ninety-three percent of adults agree that controlling who can access their personal information is important, while ninety percent agree that controlling what information is collected about them is important.[143] This makes sense; the

137. *Id.*

138. Ben Stump, *Optimizing Cell and Tower Sites During the Data Explosion*, ANTENNA SYS. & TECH. (Nov. 28, 2013, 2:50 PM), http://www.antennasonline.com/main/articles/optimizing-cell-and-tower-sites-during-the-data-explosion/.

139. *Id.*

140. Julianne Pepitone, *What Your Wireless Carrier Knows About You*, CNN (Dec. 16, 2013, 6:22 AM), http://money.cnn.com/2013/12/16/technology/mobile/wireless-carrier-sell-data/.

141. *Id.*

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

143. MARY MADDEN & LEE RAINIE, PEW RES. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE 4 (2015), http://www.pewinternet.org/2015/05/20/

aggregate of CSLI information can paint a mosaic, revealing private and intimate information about a person's life, including one's sexual relations, business dealings, and religious beliefs.[144] It is safe to assume that the average person would likely subjectively believe that this sensitive information would be kept from a third party without their knowledge or explicit consent.

While the subjective expectation prong in the *Katz* test is most likely met, the subjective standard's relevance has recently come into question.[145] The lack of judicial attention and emphasis to the subjective expectation prong in the *Katz* test suggests that it is a "phantom doctrine" and would likely have no impact on a court's ruling in a case involving CSLI.[146] Thus, whether warrantless government use of CSLI violates the Fourth Amendment will likely hinge on the second part of the *Katz* test.

### *B. Part Two of the* Katz *Test: The Objective Expectation of Privacy*

The more difficult challenge in the *Katz* analysis is to prove the objective requirement—that society recognizes the privacy expectation against the warrantless government use of CSLI as reasonable. It is often difficult to prove an objective expectation of privacy due to the amount of arbitrariness in Fourth Amendment judgments.[147] Unless there is prior precedent involving certain technologies, judges often do not have any guidance and may be unfamiliar with the technology at issue in certain cases or how that technology is used by the public.[148] Many judges are older in age, and it has been suggested that training on recent advances in technology "would enable judges to better understand the arguments presented by lawyers, testimony offered by technical witnesses, and judicial opinions forming the basis of decisional law."[149] In theory, judges should look to society as a whole to determine if there is an objective reasonable expectation of privacy; in reality, what an objective expectation of privacy actually means varies judge to judge.[150]

Society should recognize a legitimate privacy interest in CSLI because it can reveal intimate information within constitutionally protected areas, and it is

---

americans-attitudes-about-privacy-security-and-surveillance/.

144. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

145. Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113 (2015).

146. *See id.* ("The test exists on paper but has no impact on outcomes.").

147. *See* Erik Luna, *The Katz Jury*, 41 U.C. DAVIS L. REV. 839, 845–46 (2008).

148. *See Elena Kagan: Supreme Court Hasn't "Gotten To" Email*, CBS NEWS & ASSOCIATED PRESS (Aug. 21, 2013, 12:07 PM), http://www.cbsnews.com/news/elena-kagan-supreme-court-hasnt-gotten-to-email/ (quoting Justice Kagan: "The justices are not necessarily the most technologically sophisticated people.").

149. Gary Craig Kessler, Judges' Awareness, Understanding, and Application of Digital Evidence iii (2010) (unpublished Ph.D. dissertation, Nova Southeastern University), http://www.garykessler.net/library/kessler_judges&de.pdf.

150. *See* Sam Kamin & Justin Marceau, *Double Reasonableness and the Fourth Amendment*, 68 U. MIAMI L. REV. 589, 592 (2014) ("It is now possible to speak of that famous conundrum of reasonable unreasonable searches - those searches that are sufficiently unreasonable that they deprive a defendant of his right, but not so unreasonable that any remedy will be forthcoming.").

not in widespread use by the public. CSLI is collected continuously unless a phone is powered off.[151] Thus, a significant amount of CSLI is collected in areas, such as homes, that receive the fullest extent of constitutional protection.[152] In *Kyllo*, the Court held that warrantless use of a thermal imaging device to detect heat levels inside the house was a violation of the Fourth Amendment because of "intimate details" that could be revealed such as "what hour each night the lady of the house takes her daily sauna and bath."[153] Similarly, because CSLI can reveal a person's location inside a house, judges should follow the rationale in *Kyllo* in deciding CSLI cases. In *Kyllo*, the Court noted that an important factor in its decision was that the thermal imaging instruments used by the state were not widely available or used by the public.[154] Similarly, the ability to collect CSLI is not widespread or commonly used by the public.

Assuming that cell phone users have a reasonable privacy expectation in CSLI obtained without a warrant, the third-party doctrine's effect on the analysis of CSLI must be addressed. Traditionally, the third-party doctrine limits Fourth Amendment protection when information is voluntarily provided to a third party, because society does not recognize that privacy expectation as legitimate.[155]

In our modern and technological world, the third-party doctrine is flawed.[156] The advancement of technology has caused the doctrine to overreach its original purpose, resulting in the state's ability to unreasonably further invade its citizens' privacy beyond the scope afforded by the Fourth Amendment. Justice Sotomayor's concurring opinion in *Jones* suggests that the third-party doctrine may no longer be maintained, stating "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[157]

The third-party doctrine should not apply to CSLI for several reasons. First, a key component of the third-party doctrine is voluntariness; to waive Fourth Amendment protection, the production of information to a third party must be voluntary.[158] Cell phone users do not voluntarily give up CSLI in the same manner as home phone users gave up dialed phone numbers in *Smith v. Maryland*. In *Smith*, the defendant had to physically dial the phone, a voluntary activity, in order for the pen register to collect the number that was being

151. U.S. DEP'T OF HOMELAND SEC., *supra* note 16.

152. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 37–38 (2001) ("[I]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."); Payton v. New York, 445 U.S. 573, 590 (1980) (explaining that the Fourth Amendment "has drawn a firm line at the entrance to the house.").

153. *Kyllo*, 533 U.S at 38.

154. *Id.* at 40.

155. Smith v. Maryland, 442 U.S. 735, 745 (1979).

156. *See* Elspeth A. Brotherton, Comment, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 567 (2012).

157. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

158. United States v. Miller, 425 U.S. 435, 435 (1976); *Smith*, 442 U.S. at 735.

called.[159] In contrast, no voluntary action triggers CSLI collection–as long as the cell phone is powered on, the information can be extracted. In *Smith*, the user had absolute control over what information was given and when that information would be conveyed. The telephone user would manually have to input the numbers for the pen register to record the information. This is not the case with CSLI, as it is collected periodically without solicitation.[160] As the Federal District Court in *In re Tel. Info.* noted, if a cell phone user is roaming off their usual network, the seamless transition to the unknown network would result in a cell phone user not knowing the identity of the third party collecting their CSLI.[161] The cell phone user does not voluntarily take any of these actions.

Second, proponents of warrantless government CSLI collection argue that cell phone users should be aware that CSLI data is being collected, and that the act of having a cell phone is itself a voluntary act.[162] Unlike the monthly phone bill in *Smith* that provided all the numbers dialed during the billing cycle, cell phone companies do not provide customers with a list of their locations for the prior month.[163] This would suggest that customers are not aware of what information is collected and are not voluntarily disseminating that information. Therefore, the position that customers should be knowledgeable of CSPs collecting CSLI is not persuasive.

Advocates for warrantless government use of CSLI take a similar stance as Justice Alito in *Jones*; they argue that society does not recognize the privacy interest in CSLI because new technology has provided "increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."[164] This argument erodes the rights of the people, setting the precedent that the government should be granted greater power to intrude into private affairs as technology advances. While cell phones are a convenience in our society, they are far from a choice. To be a productive member of society, a cell phone has become a necessity.[165] The federal government, through the Lifeline program, also known as the "Obama Phone," has recognized the need for mobile phones by providing subsidies for free government funded cell phones to low income individuals and families.[166] The American people should

159. *Smith*, 442 U.S. at 742.

160. *See id.* at 743 (recognizing that phone companies receive numerical information from phone users and even record information for business reasons).

161. *In re* Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1028–29 (N.D. Cal. 2015).

162. *See e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013).

163. *See Smith*, 442 U.S at 742 ("All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

164. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

165. *See* Natasha Duarte, *Supreme Court Should Speak Up on Cell Site Location Information*, CTR. FOR DEMOCRACY & TECH. (Oct. 28, 2016), https://cdt.org/blog/supreme-court-should-speak-up-on-cell-site-location-information/.

166. *See* Jordan Malter, *Who Gets Rich Off 'Free' Government Phones*, CNN (Oct. 26, 2012, 10:37 AM), http://money.cnn.com/2012/10/26/technology/mobile/tracfone-free-phones/;

not lose their right to privacy because new technology exists to make their daily lives easier and more manageable.

## VII. CONCLUSION

CSLI is just one example of how, as technology continues to advance, the existence of the third-party doctrine in its current state will continue to erode the protections given under the Fourth Amendment.[167] Until the Court addresses the third-party doctrine, the public needs protection from unreasonable invasions by warrantless government searches utilizing CSLI.

The best course for implementing a remedy to provide the necessary protection would be through legislative action because elected officials more accurately reflect the will of the American people than the judiciary and there is no telling if or when the Court will provide a new standard. Although the Court will hear a CSLI case during its next term, there is no guarantee that the ruling will address the underlying problem of the third-party doctrine, once again leaving lower courts with limited guidance.[168] Instead, Congress needs to reevaluate the SCA, because much has changed since the 1980s when the act was passed and much of the intent behind the legislation has now become frustrated.[169] Congress should strike the provision requiring only reasonable suspicion and a court order to obtain CSLI. This would require law enforcement to obtain a warrant before accessing CSLI, subjecting their requests to the higher probable cause standard of proof.

Unfortunately, Congress' production in recent years has been at historic lows.[170] It cannot be certain that Congress will want to, or be able to, revise the SCA. If the federal government is unable to enact legislation to protect citizens, it is up to the individual states to fill the void. As of February 2017, thirty-three

---

RealFreedom1776, *Original Obamaphone Lady*: *Obama Voter Says Vote for Obama Because He Gives a Free Phone*, YOUTUBE (Sept. 26, 2012), https://www.youtube.com/watch?v=tpAOwJvTOio.

167. *See* Lucas Isaacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 1048 (2016) ("Controversy surrounding third party doctrine will not abide any time soon. On one side are those who believe that the protections of warrant and probable cause requirements long afforded to private information need to be extended onto the platforms where such information now resides. On the other side are those who believe that, in an era when commercial actors can assemble stunningly detailed portraits of one's relationships, habits, and proclivities, such requirements would hamstring the government in the service of providing no more than an illusory fig leaf of privacy.").

168. Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016), *cert. granted,* 137 S. Ct. 2211 (2017).

169. *See* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 275–76 (2013) (stating the purpose of the SCA was "to ensure adequate protection of electronic communications" in response to the limitations of Fourth Amendment protections).

170. Chris Cillizza, *Yes, President Obama is Right. The 113th Congress Will Be the Least Productive in History*, WASH. POST (Apr. 10, 2014), https://www.washingtonpost.com/news/the-fix/wp/2014/04/10/president-obama-said-the-113th-congress-is-the-least-productive-ever-is-he-right/.

states either have "no binding authority or explicitly allow for law enforcement to access this data without a warrant."[171] However, several states have passed legislation providing greater protection for CSLI. For example, Colorado, Maine, Minnesota, Montana, Tennessee, and Utah passed statutes expressly requiring law enforcement to apply for a search warrant to obtain CSLI.[172] Other states have passed statutes applying only towards real time or active CSLI.[173] The legislators of these states have recognized the privacy interests in CSLI and the flaws and limitations of the third-party doctrine, opting to provide protection to cell phone users instead of relying on a judicial remedy. This proactive approach is the most direct and easily obtainable remedy because courts are slow to make changes and provide much deference to *stare decisis*.

There is little doubt that government action to obtain CSLI without a warrant is an unreasonable search under the original meaning of the Fourth Amendment and the *Katz* test. CSLI has many positive uses and should continue to be utilized in appropriate manners that respect the privacy interests of the public. The benefits to the public, law enforcement, and CSPs are significant, but government need for CSLI does not outweigh the privacy interests that it would infringe upon. Stricter regulations are needed to obtain CSLI. Because both individuals and society recognize this privacy interest, the government should never be able to obtain CSLI without a warrant and must satisfy the standard for probable cause. Moreover, the third-party doctrine has been proven to have extensive flaws, resulting in further government intrusion into the personal lives of citizens and impeding the purpose behind the Fourth Amendment. CSLI has proven that it is time to reevaluate the third-party doctrine, thus requiring sweeping reforms to Fourth Amendment jurisprudence. As technology continues to advance, it is imperative that the protections afforded by the Fourth Amendment continue to evolve with the ever-changing landscape. Reevaluating the third-party doctrine and requiring warrants to obtain CSLI would be a significant step in restoring the original purpose of the Fourth Amendment in the modern age.

---

171. Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED (Feb. 2, 2017, 7:00 AM), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/.

172. *See, e.g.*, COLO. REV. STAT. § 16-3-303.5(2) (West, Westlaw through First Regular Session of the 71st General Assembly (2017)); ME. REV. STAT. tit. 16, § 648 (West, Westlaw through 2017 First Regular Session of the 128th Legislature); MINN. STAT. §§ 626A.28(3)(d), 626A.42(2) (West, Westlaw through 2017 Regular and First Special Sessions); MONT. CODE ANN. § 46-5-110(1)(a) (West, Westlaw through the 2017 session); TENN. CODE ANN. § 39-13-610(b) (West, Westlaw through the 2017 First Regular Session of the 110th Tennessee General Assembly); UTAH CODE ANN. § 77-23c-102(1)(a) (West, Westlaw through the 2017 General Session).

173. *See, e.g.*, IND. CODE § 35-33-5-12 (West, Westlaw through the 2017 First Regular Session of the 120th General Assembly); MD. CODE ANN., Crim. Proc. § 1-203.1 (West, Westlaw through the 2017 Regular Session of the General Assembly); VA. CODE ANN. § 19.2-56.2 (West, Westlaw through the end of the 2017 Regular Session); WASH. REV. CODE § 9.73.260 (West, Westlaw through the 2017 Third Regular Session of the Washington legislature); WIS. STAT. § 968.373(2) (West, Westlaw through 2017 Act 57).