Catholic University Law Review

Volume 66
Issue 3 *Spring 2017*

Article 10

6-30-2017

The Third Party Doctrine and Physical Location: The Privacy Implications of Warrantless Acquisition of Historical Cell Site Location Information

Matthew G. Baker

The Third Party Doctrine and Physical Location: The Privacy Implications of Warrantless Acquisition of Historical Cell Site Location Information

Cover Page Footnote
J.D., The Catholic University of America, Columbus School of Law, 2017; B.A., The George Washington University, 2008. The author would like to thank Professor Clifford Fishman for his guidance and expertise throughout the writing of this Comment. The author is also grateful to the staff of the Catholic University Law Review for their assistance in publishing this Comment.

THE THIRD PARTY DOCTRINE AND PHYSICAL LOCATION: THE PRIVACY IMPLICATIONS OF WARRANTLESS ACQUISITION OF HISTORICAL CELL SITE LOCATION INFORMATION

Matthew G. Baker[+]

It is very likely that the first thing you see in the morning and the last thing you see at night is the screen of your cell phone. Cell phones are owned by over ninety percent of Americans, making it the most widely adopted piece of technology in history.[1] The adoption of new technology always leads to a reexamination of how the Constitution protects the public from the probing eyes of law enforcement. The Fourth Amendment to the U.S. Constitution states in part that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[2] Cell phones are not listed in the Fourth Amendment. Does this mean that the police may search their contents without a warrant or valid warrant exception? The U.S. Supreme Court says no.[3]

If the contents of a cell phone are protected from warrantless searches, what about a record of the locations where a cell phone has traveled? The U.S. Circuit Courts of Appeals have ruled decisively that accessing historical cell site location information (CSLI) by law enforcement does not constitute a search under the Fourth Amendment.[4] Despite opportunities, the Supreme Court has

---

[+] J.D., The Catholic University of America, Columbus School of Law, 2017; B.A., The George Washington University, 2008. The author would like to thank Professor Clifford Fishman for his guidance and expertise throughout the writing of this Comment. The author is also grateful to the staff of the *Catholic University Law Review* for their assistance in publishing this Comment.

1. Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RESEARCH CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

2. U.S. CONST. amend. IV.

3. *See generally* Riley v. California, 134 S. Ct. 2473 (2014). The Court held in *Riley* that the search incident to arrest rule from *United States v. Robinson* allowing a warrantless search of a suspect for weapons or evidence of a crime did not extend to the contents of a cell phone found on a suspect at the time of arrest. *Id.* at 2483–85 (citing United States v. Robinson, 414 U.S. 218, 235–37 (1973)).

4. *See generally* United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 884, 890 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 309 (3d Cir. 2010); *see also* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 28:4 (2016) ("CSLI reveals the cell tower with which the phone is or was communicating at a particular point in time and, often, the sector within that tower's cell. This provides useful information as to the phone's location, but with several limitations.").

thus far chosen not to hear a case addressing the issue of CSLI and the Fourth Amendment.[5]

The evolution of technology has always proven challenging to the court system. In 2001, the Court developed a rule stating that if a device used by law enforcement to surveil a constitutionally protected space, such as the home, is a tool that is not generally available to the public, then a search has occurred.[6] Again, in 2012, the Court addressed the challenge technology poses in *United States v. Jones*.[7] In *Jones*, the police placed a GPS tracking device on a suspect's car without a warrant and collected location data for twenty-eight days.[8] The changes in technology that allow the police to track a suspect's location through his or her cell phone with ease raise significant and troubling implications for privacy, which courts are beginning to address.[9] Dissenting in a separate case in the Ninth Circuit, Judge Alex Kozinski argued that the United States may have reached the level of dragnet policing when a cell phone provider has to develop a self-service website for police to retrieve CSLI records "from the comfort of their desks" due to the high levels of demand.[10]

The widespread adoption of cell phones is a large part of the reason why CSLI collection is such an important issue. Accessing CSLI by law enforcement is not a trivial occurrence that is only used sparingly; in the first six months of 2015, the major cell phone carriers in the United States received tens of thousands of court orders that included demands for CSLI.[11] For example, in

---

5. *See* Davis v. United States, 136 S. Ct. 479, 480 (2015). The Court denied certiorari in the *Davis* case, likely due to the decision of the Fourth Circuit to rehear *Graham*. *Id.* at 480.

6. Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that technology used by law enforcement to detect heat emanating from the interior of a house that is not available to the general public constituted a search under the Fourth Amendment).

7. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

8. *Id.* at 402–03. Over the course of four weeks of surveillance, the police collected over 2,000 pages of data related to the location of the suspect's car. The GPS device was able to establish the location of the car within an accuracy of 50-100 feet. *Id.* at 403.

9. *See id.* at 416–17 (Sotomayor, J., concurring); United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010). Law enforcement officials understand the advantage of tracking individuals through their cell phones because the majority of adults own and regularly use cell phones, and the capability to remotely track a phone eliminates the problems associated with trying to physically install a tracking device on a vehicle. M. Wesley Clark, *Symposium on Electronic Privacy in the Information Age: Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007).

10. *Pineda-Moreno*, 617 F.3d at 1126 (Kozinski, C.J., dissenting from rehearing *en banc*). Judge Kozinski noted that while people may mask their movements by traveling at night or in large crowds, there is no hiding from the "all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention." He also noted the dense "honeycomb" of cell phone towers that can be used to track a person's location. *Id.*

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

the first half of 2015, Sprint received 24,209 court orders,[12] Verizon received 37,230 court orders,[13] and T-Mobile received 47,998 court orders (2015 totals).[14] For the second half of 2015, AT&T received 18,768 court orders and for the first half of 2016, AT&T received 16,077 court orders.[15]

The U.S. Circuit Courts of Appeals have decided that accessing historical CSLI does not constitute a search under the Fourth Amendment. Ruling *en banc* in *United States v. Graham*,[16] the Fourth Circuit held that no warrant is required.[17] The Fourth Circuit built from the Eleventh Circuit's *en banc* decision in *United States v. Davis*[18] that CSLI access does not constitute a

12. *Sprint Corporation Transparency Report*, SPRINT CORP. 1, 2 (2015), http://goodworks.sprint.com/content/1022/files/TransaparencyReportJuly2015.pdf (court orders include pen registers and trap and traces, wiretaps, and real-time location requests.)

13. *Verizon's Transparency Report for the First Half of 2015*, VERIZON CORP. (July 20, 2015), http://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/01/Verizon-Transparency-Report-2015-first-half.pdf (including general orders, pen registers, trap and trace orders, and wiretap orders).

14. *T-Mobile Transparency Report for 2013 and 2014*, T-MOBILE 1, 4 (2014), https://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf (excluding orders for wiretaps, pen register, and trap and trace).

15. *AT&T Wireless Transparency Report*, AT&T 1, 3 (July 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf.
Smaller cellular telephone companies do not retain the ability to provide the same level of information to law enforcement as the larger companies do, and many smaller companies do not keep detailed records that separate out the different types of law enforcement requests. *See generally* Letter from Robert J. Irving, Jr., Chief Legal and Admin. Officer, Cricket Wireless, to Representative Edward J. Markey (Oct. 7, 2013) (on file with author); Letter from Benjamin M. Moncrief, Director Gov't Relations, C Spire Wireless, to Representative Edward J. Markey (Oct. 7, 2013) (on file with author); Letter from John C. Gockley Vice-President Legal and Regulatory Affairs, U.S. Cellular, to Representative Edward J. Markey (Oct. 1, 2013) (on file with author).

16. 824 F.3d 421, 421–22 (4th Cir. 2016).

17. *Id.* at 424–25 ("We now hold that the Government's acquisition of historical CSLI from Defendant's cell phone provider did not violate the Fourth Amendment. Supreme Court precedent mandates this conclusion. For the Court has long held that an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to [a] third part[y].'"); *see also* Orin S. Kerr, *Fourth Circuit Grants Rehearing, Eliminates Split, On Cell-Site Surveillance*, WASH. POST: VOLOKH CONSPIRACY (Oct. 29, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/10/29/fourth-circuit-grants-rehearing-eliminates-split-on-cell-site-surveillance/.

18. 785 F.3d 498 (11th Cir. 2015).

search.[19] The Fifth,[20] Third,[21] and Sixth Circuits[22] have also held that court orders for CSLI do not require a warrant.[23]

There are two principle issues at stake in this debate. The first is whether CSLI is shareable without a warrant by cell phone service providers under the third-party doctrine.[24] The second is whether warrantless electronic surveillance over a long period of time that is undertaken without a trespass violates a suspect's, and society's, expectation of privacy.[25] CSLI should be protected by a warrant requirement due to the substantial privacy concerns at stake, such as the ability of law enforcement to track an individual's location purely through his or her cell phone.

Cell phones function by sending a radio signal from the phone to a network of base stations or cell towers.[26] Cell towers "typically face three or four different directions, and each of these individual sides to the tower are known as a cell 'site' or 'sector.'"[27] These sites "contain antennas that detect the radio signal emanating from a cell phone and connect the phone to the cellular network."[28] A cell phone that is turned on is in constant communication with the nearest cell tower to maintain a connection; there is an exchange of

19. *Id.* at 513.

20. *In re* Application of the U. S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional.").

21. *In re* Application of the U. S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010) ("In sum, we hold that CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination.").

22. United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment.").

23. *See id.*; *see also supra* notes 20–21. The debate over cell phone surveillance is multi-faceted, and this paper cannot touch on all of the relevant issues. The use of cell-site simulators, commonly known as Stingrays; real-time or prospective cell site location information; and cell tower dumps to identify specific phones in a geographic area at a specific time are each an article on their own and are outside the scope of this paper.

24. *See* 3A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE § 663 n.6 (4th ed. 2016) ("[C]ell phone users voluntarily communicate this information to cell phone companies and it is not unconstitutional for the company to provide the information to law enforcement.").

25. *See* United States v. Graham, 796 F.3d 332, 347 (4th Cir. 2015), *aff'd on reh'g*, 824 F.3d 421 (4th Cir. 2016) (en banc) (declining to address whether Katz test would be violated by the actions taken by law enforcement absent a trespass).

26. *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 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) [hereinafter Blaze Testimony]; Brief for Elec. Frontier Found. et al. as Amici Curiae Supporting Petitioner at 8, *cert denied*, Davis v. United States, 136 S. Ct. 479 (2015) (No. 15-146) [hereinafter Amici Curiae Brief].

27. Amici Curiae Brief, *supra* note 26, at 8.

28. *Id.*

information approximately every seven seconds.[29] The automated process of communication between cell tower and cell phone is known as "pinging," and it occurs with no input by the user.[30] Additionally, every time a cell phone makes or receives a phone call, sends or receives a text message, or otherwise uses cellular data, it generally connects to the nearest cell tower and the service provider makes a record of that connection and saves it to its servers.[31] Due to the proliferation of smart phones that can accomplish much more than just dial and receive calls,[32] the ability of law enforcement to collect CSLI has expanded to include information generated when applications, such as email applications, refresh in the background when the phone is idle.[33]

The fact that different kinds of CSLI are generated by cell phones and requested by law enforcement in the course of investigations has complicated matters as courts have begun to analyze this issue. For example, the Fifth Circuit and Eleventh Circuit examined cases where the only CSLI collected was generated from calls dialed and received.[34] In contrast, in a case originating in California, the government requested, and was subsequently denied, a court order for CSLI that included data points collected from applications running on the phone when it was idle and not actively being used by the owner.[35] CSLI has become increasingly accurate with the proliferation of cell towers, especially in urban areas.[36] Depending on the density of cell towers, CSLI can pinpoint an individual device to a specific room within a building.[37] This is a significant change from the introduction of cell phones in the 1980s, when CSLI could only provide an approximate location over a wide geographic area.[38]

---

29. Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. FED. 2D § 2 (2015).

30. *Lesson Plan: How Cell Phones Work*, U.S. DEP'T OF HOMELAND SEC. (2010), https://www.eff.org/document/how-cell-phones-work-powerpoint.

31. Meyer, *supra* note 11.

32. Riley v. California, 134 S. Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."); *see also* Orin S. Kerr, *Forward: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404 (2013) (noting that modern smartphones have a storage capacity equivalent to that of a home computer sold in 2004).

33. *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1027 (N.D. Cal. 2015).

34. *Id.* at 1031 (distinguishing the current case from the Fifth and Eleventh Circuits cases that examined circumstances using 2010 technology that only generated CSLI from telephone calls, as opposed to technology that can collect CSLI when the phone is idle).

35. *Id.* at 1032–33 (noting that the government's definition of a call in its application included any function, both active and passive, that facilitated a transfer of data between a phone and a cell tower, to include data from applications running in the background).

36. Blaze Testimony, *supra* note 26, at 46–47.

37. *Id.* at 44.

38. *Id.* at 43.

Under authority granted in the Stored Communications Act (SCA), law enforcement may request a court order that only requires reasonable suspicion to compel a service provider to turn over historical CSLI about a targeted phone number.[39] Law enforcement has stressed the importance of gaining access to historical CSLI during the early stages of an investigation when there may not be enough evidence to satisfy a requirement for probable cause.[40] The U.S. Circuit Courts of Appeals have appeared to rule decisively that there is no requirement for a warrant before law enforcement can access CSLI. These rulings show that a legislative fix is required to ensure the protection of the privacy of Americans.

This Comment argues that accessing cell site location information by law enforcement should require a warrant due to the vast quantity of data available when looking at historical locations. First, this Comment describes the evolution of the Fourth Amendment jurisprudence from a trespass-based test to the expectation of privacy test, and how the third-party doctrine changed society's expectations. Second, this Comment describes how the Fourth Amendment has been interpreted in cases involving the tracking of individuals by law enforcement. Third, this Comment describes a series of cases heard in U.S. Circuit Courts of Appeals relating to the historical acquisition of cell phone location information. Finally, this Comment argues for a legislative fix to require a warrant supported by probable cause before law enforcement can gain access to historical location data.

I. THE EVOLUTION OF THE FOURTH AMENDMENT AND PRIVACY

A. Phone Booths and Betting Operations: The Expectation of Privacy

The Fourth Amendment to the U.S. Constitution states in part that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[41] Prior to the 1960s, physical trespass was required before a court would rule that a search had occurred, as "protection of property rights against government interference" was paramount in Fourth Amendment jurisprudence.[42] The landmark 1967 case of

39. 18 U.S.C. § 2703(d) (2012) ("A court order for disclosure . . . shall issue only if the governmental entity offers 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.").

40. *Geolocation Technology and Privacy: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 2 (2016) (statement of Richard Downing, Deputy Assistant Att'y Gen. of the United States).

41. U.S. CONST. amend. IV.

42. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004) (noting that the Fourth Amendment was enacted to protect property rights in response to actions of the British prior to the Revolutionary War and that courts interpreted the Amendment to protect against government trespass).

Katz v. United States[43] gave us Justice Harlan's concurring opinion describing the reasonable expectation of privacy standard that has become the bedrock of search doctrine under the Fourth Amendment.[44] *Katz* dealt with the placement of a listening device on the outside of a phone booth by the FBI that allowed them to listen to one side of phone conversations that took place within the booth.[45] Relevant to Fourth Amendment precedent at the time, the listening device did not require any physical trespass into the booth in order to function and thus was not considered a search.[46] The Harlan Test asks whether an individual has a subjective expectation of privacy in the activity the individual is engaged in, and if society finds that expectation reasonable.[47] In *Katz*, the Court stated "the Fourth Amendment protects people, not places,"[48] when it moved away from the trespass doctrine that had previously governed search jurisprudence.[49] Relevant to CSLI, the Court in *Katz* held that people have an expectation to be free of a government search in actions that they take, not in relation to where they are located.[50]

B. False Friends and Pen Registers: The Third-Party Doctrine

On multiple occassions, the Supreme Court has held that information conveyed by a defendant to a third party has no reasonable expectation of privacy, even if the defendant has reason to believe that his confidence will not

43. 389 U.S. 347 (1967).

44. *Id.* at 360–61 (Harlan, J., concurring). In *Florida v. Jimeno*, Chief Justice Rehnquist wrote that "[t]he touchstone of the Fourth Amendment is reasonableness," echoing Justice Harlan's concurrence in *Katz* and demonstrating that the reasonableness analysis is an integral part of Fourth Amendment jurisprudence. Florida v. Jimeno, 500 U.S. 248, 250 (1991).

45. *Katz*, 389 U.S. at 348–49 ("[T]he Court of Appeals rejected the contention that the recordings had been obtained in violation of the Fourth Amendment, because '(t)here was no physical entrance into the area occupied by, (the petitioner).'").

46. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511–12 (1961) (holding that the use of a spike mike that physically intruded into the petitioner's home was a violation of the Fourth Amendment); Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding that information heard by use of a detectaphone was not a violation of the Fourth Amendment as any trespass necessary to set up the listening device was not material in the use of the detectaphone); Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that the placing of a wiretap on the phone lines outside of a home does not constitute a search under the Fourth Amendment because there was no physical intrusion into the home or curtilage).

47. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Despite only being a concurrence, and not the holding in the case, the Harlan Test has become the bedrock of Fourth Amendment jurisprudence regarding whether a search has occurred in circumstances when there is not a physical intrusion onto the property of the suspect.

48. *Id.* at 351.

49. *Cf.* Kerr, *supra* note 42, at 818, 820 (noting that prior to *Katz*, the courts adopted a strict property rights view of the Fourth Amendment, where a trespass was necessary for a search to have occurred).

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

be betrayed.[51] The third-party doctrine developed around a series of false friend cases that challenged the use of informants to obtain evidence against criminal defendants.[52] In *United States v. White*,[53] a criminal case, the defendant challenged the use of an informant wearing a wire while speaking with a suspect as violating his expectation of privacy.[54] The Court held that White assumed the risk that any information he divulged to someone else could be shared with law enforcement.[55]

In *United States v. Miller*,[56] The third-party doctrine made a leap from conduct involving government informants to conduct of corporations that had business dealings with defendants.[57] The Court found that information concerning a depositor's accounts shared by a financial institution with the police in response to a subpoena did not constitute a search under the Fourth Amendment.[58] The Court reasoned that bank records, such as checks and deposit slips, were not private papers, but rather documents for use in commercial transactions that were not protected by the Fourth Amendment.[59]

The 1979 case of *Smith v. Maryland*[60] held that a pen-register[61] placed on a phone line by the phone company at the request of the police did not constitute a search under the Fourth Amendment because there is no expectation of privacy in information voluntarily shared by a customer with the telephone company.[62] Additionally, the Court held that because customers "voluntarily" share the identity of phone numbers dialed with the phone company, they assume the risk that the information will be shared with the police because there is no

51. Smith v. Maryland, 422 U.S. 735, 742–43 (1979); United States v. Miller, 425 U.S. 435, 443 (1976) (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)).

52. *See, e.g.*, *Miller*, 425 U.S. at 440 (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)); United States v. White, 401 U.S. 745, 752–53 (1971).

53. 401 U.S. 745 (1971).

54. *Id.* at 746–47.

55. *Id.* at 752 ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police.").

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

57. *Miller*, 425 U.S. at 444 (holding that the issuance of a subpoena to a third party for the records of a defendant does not violate the Fourth Amendment even if a criminal prosecution is possible).

58. *Id.* at 440.

59. *Id.* at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

60. 442 U.S. 735 (1979).

61. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 570 (2009) ("A pen register was a device installed at the phone company to record the numbers dialed from a specific telephone.").

62. *Smith*, 442 U.S. at 742–43 (robbery suspect dialed the phone numbers on his home telephone).

expectation of privacy in any information shared with a third party.[63] Foreshadowing the issues related to privacy concerns and telephones, Justice Marshall's dissent in *Smith* highlighted that even absent the contents of phone calls, the information solely illuminated by the numbers dialed has grave implications for privacy as it can provide a clear picture of an individual's lifestyle and habits.[64]

C. Barrels of Trouble and in Hot Water: Tracking Chemical Barrels with Radio Transmitters and Using Thermal Imagers on the Home

In 1983, the Supreme Court in *United States v. Knotts*[65] examined the tracking of an individual's location in the context of the Fourth Amendment.[66] The defendants in *Knotts* were suspected of purchasing chemicals to manufacture narcotics.[67] With the assistance of a chemical manufacturing and sales company, the police installed a radio transmitter in a chemical barrel that was subsequently sold to the defendants.[68] Using the radio transmitter, the police tracked the defendants to a cabin where they discovered a narcotics manufacturing lab.[69] The defendants appealed their convictions, arguing that the use of the radio transmitter to track their locations without a warrant was a violation of their expectation of privacy under the Fourth Amendment.[70]

The Court's holding was consistent with past Fourth Amendment cases — that there was a lower expectation of privacy in the movements of a vehicle on public streets.[71] The Court equated the use of a radio transmitter to following a vehicle on roads and highways using visual surveillance.[72] Despite the use of electronic means to track the location of criminal suspects, the Court made no distinction in the privacy expectation between police following the suspects and

---

63. *Id.* at 744 ("In doing so, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

64. *Id.* at 751 (Marshall, J., dissenting) (highlighting the potential for a chilling effect on First Amendment rights by those fearful of government surveillance of telephone data).

65. 460 U.S. 276 (1983).

66. *Id.* at 277.

67. *Id.* at 278.

68. *Id.*

69. *Id.* at 278–79.

70. *Id.* at 279 (noting that the Eighth Circuit held that the warrantless tracking of the chemical barrel was a violation of the defendants' expectation of privacy).

71. *Id.* at 281; *see, e.g.*, Rakas v. Illinois, 439 U.S. 128, 153–54 (1978) (Powell, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976); Cardwell v. Lewis, 417 U.S. 583, 590 (1974). In his concurrence in *Rakas*, Justice Powell noted "[n]othing is better established in Fourth Amendment jurisprudence than the distinction between one's expectation of privacy in an automobile and one's expectation when in other locations." *Rakas*, 439 U.S. at 153–54 (Powell, J., concurring).

72. *Knotts*, 460 U.S. at 281 ("A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view." (quoting *Cardwell*, 417 U.S. at 590)).

the use of a radio transmitter to track the location of a barrel of chemicals in the suspects' possession.[73]

The following year, the Court heard *United States v. Karo*,[74] which built upon the holding in *Knotts*, but established important limits in the use of radio transmitters to track the locations of criminal suspects.[75] In circumstances similar to *Knotts*, the government received information that criminal suspects intended to purchase chemicals to manufacture narcotics.[76] With the assistance of the business selling the chemicals, the government installed a radio transmitter in one of the chemical barrels.[77] The government used the radio transmitter to track the chemical barrels and the suspects to a number of different locations, including public storage facilities and private residences.[78] In a notable departure from *Knotts*, prior to the execution of a search warrant on the residence where the government believed narcotics were located, the government verified that the chemical barrel was inside the house through the use of the radio transmitter.[79]

The Court held that there were significant privacy concerns implicated with tracking items within a residence. It held that the surreptitious use of a radio transmitter to verify the location of an item at a particular time was a violation of the Fourth Amendment because law enforcement could not verify the information by visual observation from outside the curtilage of the home.[80]

In 2001, the Court ruled on *Kyllo v. United States*[81] and developed a rule to help deal with changes in technology and its effects on the Fourth Amendment.[82] Under suspicion that the defendant was growing marijuana inside his home, federal agents used a thermal imaging device to measure the temperature of the

---

73. *Id.* at 282 (noting that the use of a beeper to track the barrel is no different than using visual surveillance to follow it on public roads).

74. 468 U.S. 705 (1984).

75. *Id.* at 713–15.

76. *Id.* at 708.

77. *Id.* With the help of an informant, the government substituted one of the barrels with a barrel of their own that contained a radio transmitter. Using a combination of visual surveillance and the radio transmitter, the government tracked the location of the barrel. *Id.*

78. *Id.* at 708–10. The Court took particular offense at the use of the beeper within the home of the suspect, noting, "[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Id.* at 714.

79. *Id.* at 709–10. The government used the installed radio transmitter over the course of three days to verify that the chemical barrels were still located in the house of the suspects. *Id.*

80. *Id.* at 714–15. The curtilage is defined as an area near the home that is "so intimately tied to the home itself" that it is given the same protection as if it was within the home. United States v. Dunn, 480 U.S. 294, 301 (1987).

81. 533 U.S. 27 (2001).

82. *Id.* at 34 (holding that the use of technology not generally available to the public to gather information regarding the interior of the home is a search under the Fourth Amendment).

outside of the home to determine if excessive heat was emanating from it.[83] Based off of the temperature readings and other information, the government secured a search warrant and discovered a marijuana growing operation.[84] The Court determined that the use of the thermal imager on the outside of the home constituted a search under the Fourth Amendment.[85] The Court recognized that changing technology affected privacy and that the law had to adapt to ensure constitutional protections.[86] The Court developed a rule stating that the use of technology that is not in common usage by the public to learn details of the home, unknowable without a physical intrusion, is considered a search and presumed to be unreasonable without a warrant.[87]

D. Search in the Age of Phones and GPS: Jones *and* Riley

The Court began to address the privacy implications of tracking the movements of individuals in *United States v. Jones*,[88] when it heard a case concerning the use of a GPS tracker by the police to follow a drug-dealing suspect for twenty-eight days.[89] The majority focused on the physical actions of law enforcement when installing the GPS tracking device on the defendant's vehicle; the police meaningfully interfered with the property rights of the defendant in violation of the trespass doctrine of the Fourth Amendment.[90] Justice Sotomayor emphasized in her concurrence that the ability to easily collect and store vast quantities of location data about an individual without a warrant could have grave consequences for the freedom of expression and association if the public believes that the government is closely tracking their movements, and could very easily be susceptible to abuse by the police.[91]

Justice Alito's concurrence, on the other hand, focused on how long a time period the police can track an individual without a warrant before it becomes unreasonable.[92] Justice Alito argued that there is an expectation from the public

---

83. *Id.* at 29–30. The government took temperature readings of the suspect's house and neighboring houses for comparison. *Id.* at 30.

84. *Id.* at 30.

85. *Id.* at 40.

86. *Id.* at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

87. *Id.* at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

88. 565 U.S. 400 (2012).

89. *Id.* at 402–03.

90. *Id.* at 404–05 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

91. *Id.* at 416 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

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

that the police would not secretly track the movements of an individual for four weeks without a warrant.[93] While he did not suggest a bright line rule of how long is too long, he stated unequivocally that four weeks is too long.[94] In a likely prelude to issues related to location tracking of cell phones, Justice Alito highlighted that placing a GPS device on a car is not necessary for the police to track an individual's every movement.[95] Modern cell phones come equipped with GPS devices, and even older cell phones can be tracked through their interaction with cell towers.[96]

Justice Sotomayor's concurrence in *Jones* seems to cautiously embrace the idea of the mosaic theory of the Fourth Amendment when she described the complete picture of a person's life that GPS monitoring can convey to law enforcement.[97] The mosaic theory states that the Fourth Amendment is implicated when law enforcement collects too much information without a warrant;[98] each incremental step may be constitutional, but taken together as a whole, they violate the Fourth Amendment.[99] The mosaic theory allows information that may appear unimportant to the uniformed viewer to appear of great importance to someone with a complete understanding of the context in which the information was collected.[100] Critics of the mosaic theory point out the inherent inconsistencies that will occur when judges are required to determine how much information is too much on a case-by-case basis, and that any arbitrary bright line rule will either be over inclusive or under inclusive.[101]

While not directly tied to location data found through cell phone interaction with cell towers, the 2014 case of *Riley v. California*[102] marked a change in how cell phones are perceived by the courts.[103] *Riley* came before the Court on a challenge to law enforcement's ability to search cell phones during a search incident to arrest.[104] The Court held that in the absence of exigent

93. *Id.*

94. *Id.* ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

95. *Id.* at 428.

96. *Id.* at 428–29 ("The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

97. *Id.* at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

98. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013).

99. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).

100. *See* CIA v. Sims, 471 U.S. 159, 178 (1985); Gray & Citron, *supra* note 98, at 71–72.

101. Gray & Citron, *supra* note 98, at 71.

102. 134 S. Ct. 2473 (2014).

103. *Id.* at 2485 (noting the difference between the search of an individual incident to arrest and the search of a cell phone during an arrest).

104. *Id.* at 2484. *Chimel v. California* in 1969 and *United States v. Robinson* in 1973 defined the scope of a search incident to arrest. The holding in *Chimel* stated that the police may search a

circumstances, it was a violation of the Fourth Amendment for the police to search a cell phone incident to arrest without a warrant.[105] The Court reasoned that the search incident to arrest doctrine was developed to ensure a police officer's safety during an arrest, and that there was little chance of the digital contents of a cell phone posing any danger to police.[106] The Court also noted that there are significant privacy concerns in allowing the police to search the digital contents of a cell phone without a warrant, in light of the large quantities of data that can easily be stored on modern cell phones.[107]

E. Legislating Electronic Searches: The Electronic Communications Privacy Act

Against the backdrop of the changing requirements of search doctrine under the Fourth Amendment, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986.[108] Title II of the ECPA is known as the Stored Communications Act (SCA), which governs police conduct in relation to accessing information from communications providers about subscribers.[109] Section 2703(d) of the SCA mandates that police apply for court orders to gain access to any stored records held by communications providers.[110] Law enforcement officers (local, state, and federal) need only a reasonable suspicion that stored noncontent communications or information stored by a communications provider is relevant and material to a criminal investigation.[111] The SCA does not require that the government show probable cause in order to access CSLI. All that is needed is a showing of "specific and articulable facts showing that there are reasonable grounds to believe" that criminal activity is associated with the communications records sought by police.[112] The SCA does

---

suspect's person and immediate grabbing area for weapons or evidence to ensure officer safety and prevent the destruction of evidence. Chimel v. California, 395 U.S. 752, 762–63 (1969). *Robinson* further defined the rule by allowing police to conduct a more thorough search of a suspect even if there is no immediate concern for the loss of evidence. United States v. Robinson, 414 U.S. 218, 236 (1973).

105. *Riley*, 134 S. Ct. at 2485.

106. *Id.* at 2484–85 (holding that the potential for destruction of evidence or harm to police is unlikely in the context of digital data stored on a cell phone).

107. *Id.* at 2489 (noting that the storage capacity of modern cell phones makes them more akin to computers than standard phones and that they can store immense quantities of data).

108. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 28 U.S.C.); *see also* Bob Davis, *Eavesdropping Looms as a Problem as Cellular-Telephone Use Widens*, WALL ST. J., Oct. 29, 1986, at 31.

109. Stored Communications Act, 18 U.S.C. § 2703 (2012).

110. *Id.* § 2703(d).

111. *Id.*

112. *Id.*; Lode, *supra* note 29, § 2. The standard required for a section 2703(d) order is significantly broader than that required for a warrant. Law enforcement may seek "any information that is materially relevant to an ongoing investigation." Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 696 (2011). This

not specifically state that CSLI falls under its jurisdiction, which is understandable as the statute was passed in 1986 prior to the wide proliferation of cell phones.[113] The information about a user collected by a communications provider includes the location of each cell phone tower that a user connects to when making or receiving phone calls and sending or receiving text messages.[114]

Despite the lack of a warrant requirement, or more likely because of it, state legislatures have begun passing their own versions of the ECPA that mandate a warrant for access to CSLI.[115] In early October 2015, California became the largest state to pass its own version of the ECPA, the California Electronic Communications Privacy Act (CalECPA), which mandates a warrant for state law enforcement access to any CSLI, as well as metadata and information stored on a device or in the cloud.[116] The passage of state data privacy laws are important because, while state statutes are not dispositive of the issue, they give an idea of what citizens of the states are willing to find reasonable.[117]

F. Reasonable Grounds vs. Probable Cause

In order to access CSLI, law enforcement is required to obtain a court order under the SCA.[118] The SCA merely requires a showing of specific facts that demonstrate that there is a reasonable belief by law enforcement that the

broad standard could allow the acquisition of data unrelated to the evidence of a crime that will aid the investigation in some manner. *Id.* at 696–97.

113. At the time of the passage of the Stored Communications Act, cell phones had only been on the commercial market for three years and were not readily available to the public due to their prohibitive cost. *See In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *6 (S.D.N.Y. Jan. 13, 2009).

114. *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113 Cong. 6 (2013) (statement of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP).

115. *See generally* Shahid Buttar, *California Leads the Way in Digital Privacy*, ELEC. FRONTIER FOUND. (Oct. 21, 2015), https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy.

116. CAL. PENAL CODE § 1546.1 (West 2016); *see also* Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED MAGAZINE (Oct. 8, 2015, 9:58 PM), http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ (noting that California is the first state to protect location data, content, metadata, and device searches).

117. *See* United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010) (noting that the decisions of state courts while not conclusive evidence, are indicative of societal understanding); *see also* Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014) (holding that using CSLI to track a suspect's cell phone for two weeks without a warrant, but with a 2703(d) order, constituted an unlawful search). On remand the district court, and subsequently the Massachusetts Supreme Court, held that the police had probable cause to obtain the historical CSLI and that the evidence could be admitted at trial. Commonwealth v. Augustine, 35 N.E.3d 688, 697–98 (Mass. 2015).

118. 18 U.S.C. § 2703(d) (2012).

information sought is relevant or material to an ongoing investigation.[119] This is a lower standard than the requirement for a search warrant, which must be supported by probable cause.[120] The courts have interpreted probable cause to mean that police, using the facts available to them, have a reasonable belief that contraband or evidence of a crime is present in the place to be searched.[121]

G. Circuit Courts and CSLI: Where We Stand Today

Five U.S. Circuit Courts of Appeals have heard challenges to the warrantless collection of CSLI by law enforcement.[122] All have ruled that the acquisition of historical location information does not constitute a search under the Fourth Amendment.[123] Panels of the Fourth and Eleventh Circuits ruled that the collection of CSLI constituted a search; the decisions were vacated and reheard *en banc*.[124] On rehearing, both courts reversed themselves and held that CSLI acquisition did not require a warrant.[125] In April 2016, the Sixth Circuit ruled, in *United States v. Carpenter*,[126] that the government does not need a warrant to acquire CSLI in the course of an investigation.[127] The Sixth Circuit based its holding on the third-party doctrine; specifically, that CSLI constitutes business records created by the cell phone carrier.[128] The court reasoned that any cell phone customer must know that when a cell phone is used it connects to the

119. *Id.*

120. U.S. CONST. amend. IV ("[N]o warrants shall issue, but upon probable cause . . . .").

121. Florida v. Harris, 133 S. Ct. 1050, 1055 (2013) (citing Texas v. Brown, 460 U.S. 730, 742 (1983)).

122. *See* United States v. Graham, 796 F.3d 332, 338 (4th Cir. 2015); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 305 (3d Cir. 2010).

123. *See Graham*, 796 F.3d at 360–61; *Davis*, 785 F.3d at 518; *Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 615; *Application of the U.S. for an Order Directing a Provider to Disclose*, 620 F.3d at 313; *see also* Meyer, *supra* note 11.

124. United States v. Graham, 624 F. App'x 75, 75 (4th Cir. 2015), *reh'g granted en banc*, *Graham*, 796 F.3d at 360–61 ("Specifically, we conclude that the government's procurement and inspection of Appellants' historical CSLI was a search, and the government violated Appellants' Fourth Amendment rights by engaging in this search without first securing a judicial warrant based on probable cause."); United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) ("In short we hold that cell site location information is within the subscriber's reasonable expectation of privacy.").

125. United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016) ("Applying the third-party doctrine, consistent with controlling precedent, we can only conclude that the Fourth Amendment did not protect Sprint/Nextel's records of Defendant's CSLI."); *Davis*, 785 F.3d at 513 ("Following controlling Supreme Court precedent most relevant to this case, we hold that the government's obtaining a § 2703(d) court order for production of MetroPCS's business records at issue did not constitute a search and did not violate the Fourth Amendment rights of Davis.").

126. 819 F.3d 880 (6th Cir. 2016).

127. *Id.* at 890.

128. *Id.* at 888–89.

nearest cell tower and conveys his location for use by the cellular provider. As such, *Smith* was binding precedent that the court was required to follow.[129]

The Third Circuit ruled in 2010 on an appeal of a denied application for an order under section 2703(d) of the SCA and held that the reasonable articulable facts standard in the statute was sufficient to justify release of the CSLI.[130] While the Third Circuit ultimately sided with the government and vacated the magistrate judge's denial of a section 2703(d) order, the court noted that the Electronic Frontier Foundation's brief argued that a cellular phone user does not voluntarily share location information with a service provider in any meaningful way.[131] The court's decision ultimately rested on statutory construction instead of privacy grounds, but it did note that Federal Communications Commission regulations mandated that by 2012 phone carriers have the ability to locate phones within 100 meters for 67% of calls and within 300 meters for 95% of calls.[132]

In a similar circumstance in 2013, the Fifth Circuit held that a magistrate judge did not have the discretion under the SCA to require a warrant when the government sought access to sixty days of CSLI generated when the phone both sent a signal for a call and was in an idle state.[133] The Fifth Circuit crafted its decision to sidestep the constitutional issues and focused solely on the statutory construction of the SCA by holding that, so long as the government met the statutory burden of proof, then the application could not be denied.[134] The Fourth and Eleventh Circuits made *en banc* decisions that are the most prominent defenses of warrantless acquisition of CSLI through implication of the third-party doctrine by holding that any location data shared with the cell phone carrier by the customer has no expectation of privacy under the Fourth Amendment.[135]

---

129. *Id.* at 888.

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

131. *Id.* at 317–18 ("[T]he only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." (quoting Amici Curiae Brief, *supra* note 26, at 21)).

132. *Id.* at 317–18 (citing 47 C.F.R. § 20.18(h)(1) (2016)).

133. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010).

134. *Application for Historical Cell Site Data*, 724 F.3d at 615 (holding that so long as the government meets the statutory standard of the Stored Communications Act, then a magistrate judge does not have the choice to deny an application for a CSLI order).

135. United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016); United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

II. ANALYZING THE ELEVENTH CIRCUIT AND FOURTH CIRCUIT CONCLUSIONS

A. The Eleventh Circuit Sides With the Third-Party Doctrine

The most prominent case holding that the collection of CSLI does not constitute a search under the Fourth Amendment is the *en banc* rehearing of *United States v. Davis*.[136] Quartavius Davis was convicted of armed robbery stemming from seven robberies that took place between August and October 2010 in the Miami, Florida area.[137] In addition to eyewitness testimony, the prosecution introduced evidence that purported to show cell phone activity by Davis in close proximity to the locations of six of the seven robberies around the time the crimes were committed.[138]

In *Davis*, a panel of the Eleventh Circuit held that the collection of CSLI by the police without a warrant was a violation of Davis' Fourth Amendment rights.[139] The *Davis* panel used the reasoning from Justice Sotomayor's concurrence in *Jones* to rule that Davis had a reasonable expectation of privacy in the location of his cell phone.[140] The panel pointed out that while there is no reasonable expectation of privacy in committing a crime, in this case the location data only showed that Davis was in the area of where a crime was committed.[141] Under that logic, Davis could be implicated for being near the scene of any crime that is committed nearby or near any number of locations in which he wished to keep his presence private.[142]

The *Davis* panel distinguished Davis' case from *Jones* by noting that in this case the tracking device was not just in Davis' automobile, as it was in *Jones*, but essentially on his person, as a cell phone tends to travel wherever its owner goes.[143] An event that a person believed to be private, such as a visit to a doctor or a rendezvous with a mistress, could suddenly be public thanks to government access to CSLI.[144] Because very private information could potentially be discovered in the course of cell phone tracking, the court held that there was no need for a mosaic of location information to be collected before there was an expectation of privacy; individual data points required protection.[145]

---

136. *Davis*, 785 F.3d at 511. The *en banc* court noted that the call records at issue belonged to the phone company for their own business purposes, not to the customer, and that there was no expectation of privacy in a customer's phone knowingly transmitting a caller's location to the nearest cell tower in order to make a call. *Id.*

137. *Id.* at 500.

138. United States v. Davis, 754 F.3d 1205, 1209–10 (11th Cir. 2014).

139. *Id.* at 1217. ("In short, we hold that cell site location information is within the subscriber's reasonable expectation of privacy.").

140. *Id.* at 1215.

141. *Id.* at 1216.

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.* at 1215–16 ("Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one.").

Following the decision of the three-judge panel in 2014, the Eleventh Circuit reheard the case *en banc* following an appeal by the government.[146] On appeal, the court held that Davis had no expectation of privacy in the data collected by his cell phone company each time he made a call due to the third party doctrine.[147] The court held that the third party doctrine from *Smith* and *Miller* controlled in this case, as Davis had no ability to assert ownership over the business records collected by his cell phone company.[148] The *en banc* court distinguished Davis' case from *Jones* by noting that the data collected by CSLI was significantly less accurate than a GPS device placed on a vehicle, and noted that a section 2703(d) order under the SCA required a level of judicial scrutiny to prevent government abuse.[149] Following the reversal of the Eleventh Circuit's panel ruling, Davis petitioned the Supreme Court for a writ of certiorari.[150] The Court denied certiorari in November 2015.[151]

B. The Fourth Circuit Follows the Lead of the Eleventh Circuit

In April 2016, the Fourth Circuit Court of Appeals, sitting *en banc*, held that no warrant is required when law enforcement seeks CSLI information under the SCA.[152] The *en banc* ruling reversed a Fourth Circuit decision from August 2015 that ruled the collection of CSLI by the police without a warrant was a violation of the Fourth Amendment.[153] In circumstances similar to *Davis*,[154] Aaron Graham was convicted of committing six armed robberies in and around Baltimore, Maryland.[155] During the investigation, police obtained a court order for CSLI records from July 2010 to February 2011, for a total of 221 days.[156] This data contained 20,235 individual location data points related to Graham's and his co-defendant's locations.[157] The district court denied a motion to suppress the CSLI evidence because the judge held that CSLI constitutes business records under the third-party doctrine and there is no expectation of privacy in records voluntarily shared with a third party.[158] The district court judge ruled that based on no clear judicial decision on the constitutionality of

146. United States v. Davis, 573 Fed. App'x 925, 925 (11th Cir. 2014) (*reh'g granted en banc* and *vacated*).

147. United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015).

148. *Id.*

149. *Id.* at 515–17 (distinguishing CSLI from GPS to determine the location of a target).

150. Petition for Writ of Certiorari, *Davis*, 785 F.3d 498 (No. 15-146).

151. Davis v. United States, 136 S. Ct. 479, 480 (2015).

152. United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016).

153. *See id.* at 424–25.

154. *Davis*, 785 F.3d at 500.

155. United States v. Graham, 796 F.3d 332, 338–39 (4th Cir. 2015).

156. *Id.* at 341.

157. United States v. Graham, 846 F. Supp. 2d 384, 387 (D. Md. 2012).

158. *Id.* at 389 ("[C]ourts have concluded that because people voluntarily convey their cell site location data to their cellular providers, they relinquish any expectation of privacy over those records.").

collecting CSLI without a warrant, the SCA provided adequate privacy protections.[159] Echoing Justice Alito in *Jones*, the court held that changing technological circumstances was an issue for the legislative branch to address.[160]

The initial panel of the Fourth Circuit based its holding in part on disagreeing with the district court's reading of Graham's cellular service provider's privacy policy that each subscriber must agree to in order to have cell phone service.[161] The policy stated that the company collected information related to when a device was in use, how it was functioning, what websites were visited, and where it was located.[162] The court discounted that the privacy policy served as a notification removing Graham's reasonable expectation of privacy in his movements and location for two reasons: (1) the policy said nothing about sharing any CSLI with the government, and (2) subscribers rarely read terms of service; thus, companies cannot expect the privacy policy to serve as notice of a lack of privacy.[163] The court distinguished the case from the third-party doctrine cases of *Smith* and *Miller* by noting that Graham and his co-conspirators did not voluntarily convey their CSLI to their service providers.[164]

Rehearing the case *en banc*, the full court held that the third-party doctrine controlled and did not require law enforcement to obtain a warrant before accessing CSLI.[165] The court stated that the holdings in *Karo*, *Kyllo*, and *Jones* all involved actions taken by the government without the assistance of third parties and could not provide any insight into whether there is a reasonable expectation of privacy in information provided by third parties.[166] The court emphasized that its holding was in agreement with every other Circuit Court that had heard similar cases and that the defendant's theory of how the government violated the Fourth Amendment was never adopted by other courts.[167] The defendant argued that an individual must "voluntarily convey" information to a third party and that in the context of CSLI there was no information affirmatively

159. *Id.* at 389–90 ("Congress in enacting the [SCA], has chosen to require only 'specific and articulable facts' in support of a government application for such records.").

160. *Id.* at 390.

161. *Graham*, 796 F.3d at 345.

162. *Id.* (The Sprint/Nextel privacy policy stated, in part, that the "[i]nformation we collect when we provide you with Services includes . . . where [your device] is located . . . .").

163. *Id.* ("First, the policy only states that Sprint/Nextel collects information about the phone's location—not that it discloses this information to the government. . . . Second, studies have shown that users of electronic communications services often do not read or understand their providers' privacy policies.").

164. *Id.* at 352–54. The court noted that CSLI is not conveyed by a customer to the cell phone provider, and the information is automatically generated when a call is placed or received. The automatic generation of the CSLI signals an involuntary act that does not implicate the third-party doctrine. *Id.* at 354.

165. United States v. Graham, 824 F.3d 421, 424–25 (4th Cir. 2016) ("[T]he third-party doctrine . . . applies even when 'the information is revealed' to a third-party, as it assertedly was here.").

166. *Id.* at 426.

167. *Id.* at 428.

conveyed by the cell phone customer to the cell phone provider.[168] The court rejected this approach in favor of the idea that the customer conveys CSLI to the provider when the cell phone exchanges signals with the nearest cell tower.[169] The court did not address what actions—automatic or otherwise—a customer must take to convey a signal to a cell tower.

C. Analyzing the Fourth and Eleventh Circuit Third-Party Doctrine Rationales

The Fourth and Eleventh Circuit *en banc* decisions relied solely on the fact that precedent under the third-party doctrine controls the ability of the government to access information voluntarily conveyed to a third party.[170] In *Davis*, the Eleventh Circuit relied on the holdings in *Miller* and *Smith* to show that the creation of CSLI by a service provider is akin to the retention of bank documents or the use of a pen-register to track numbers dialed by a specific phone line.[171] The court's analysis relied on the fact that Davis voluntarily shared his location with his service provider, and thus implicated the third-party doctrine each time he made a call by the physical act of dialing or answering a phone call.[172]

The Fourth Circuit relied on the same rationale when it reheard *Graham en banc*, stating explicitly that the third-party doctrine controlled and that the court was bound by Supreme Court precedent.[173] Additionally, the Fourth Circuit contrasted the purely governmental actions in *Jones* with the records collection by the cell phone companies to show that while there may be an expectation of privacy in government data collection, it cannot prevent the sharing of information collected and maintained by third parties.[174]

---

168. *Id.* at 429. The dissent notes that every third-party doctrine case contains two distinct sets of action taken by defendants: (1) "knowledge of particular information," and (2) "an action submitting that information." *Id.* at 443. The dissent argues that those two steps are missing from the facts in *Graham* as it is unclear what knowledge cell phone users have of the conveyance of CSLI and CSLI is an automatic function created by cell phone providers that customers do not participate in. *Id.* at 443–45.

169. *Id.* at 429 ("The [service] provider only receives . . . [CSLI] information when a cell phone user's phone exchanges signals with the nearest available cell tower.").

170. *See id.* at 437–38; *see also* United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

171. *Davis*, 785 F.3d at 511–12 (equating the retention of CSLI by a service provider with the retention of bank statements or a record of phone numbers dialed).

172. *Id.* at 512 ("The longstanding third-party doctrine plainly controls the disposition of this case.").

173. *Graham*, 824 F.3d at 436 (noting that the defendants raised the same issues as the dissent in *Smith*, but as that did not sway the majority of the Supreme Court in 1979, it cannot sway the circuit court in 2016).

174. *Id.* at 435.

III. DUE TO CHANGING TECHNOLOGY A WARRANT MUST BE REQUIRED TO ACCESS CSLI

A. The Possibility of a Judicially Created Rule

It appears extremely unlikely that the U.S. Supreme Court will decide the CSLI issue due to the lack of a circuit split and the near uniform legal analysis used by the courts, despite the increasing understanding of how substantive a picture CSLI information can provide about an individual's movements and life.[175] If the Court chooses to hear a case dealing with the use of CSLI without a warrant, it should use the groundwork that was laid in the *Jones* decision to require a warrant supported by probable cause before giving law enforcement access to historical CSLI.[176] The *Katz* expectation of privacy analysis clearly supports the requirement for a warrant,[177] as it can reasonably be inferred that there is both a subjective and objective expectation of privacy in the historical locations visited by a cell phone and by extension, its owner. As Justice Alito noted in his concurrence in *Jones*, the prolonged collection of location information about a subject has grave concerns for privacy.[178] He noted that with the facts presented in the case, the continuous monitoring of a suspect's vehicle with a GPS device for twenty-eight days was unconstitutional. But he did not draw a bright line rule stipulating what, if any, length of time would be constitutional absent a warrant.[179]

The police in the *Graham* and *Davis* cases acquired 221 and 67 days of CSLI, respectively.[180] Even without a bright line rule, it would appear that the number of days of activity examined by the police would violate Justice Alito's rule that four weeks of activity was too long without a warrant. While it is clear that the collection of multiple months of location data is a violation of the Fourth

---

175. Tim Cushing, *Government Asks Appeals Court to Change Its Mind on Warrant Requirement for Cell Site Location Info*, TECHDIRT (Sept. 21, 2015, 1:49 PM), https://www.techdirt.com/articles/20150919/09323432295/government-asks-appeals-court-to-change-mind-warrant-requirement-cell-site-location-info.shtml.

176. *See generally* United States v. Jones, 565 U.S. 400, 407, n.3 (2012) ("Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred."); Riley v. California, 134 S. Ct. 2473, 2483, 2485 (2014) (concluding that *Robinson*, which held that no additional justification is needed for a warrantless search of a person incident to a lawful arrest, is not extended to the search of cell phones).

177. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

178. *Jones*, 565 U.S. at 430 (Alito, J., concurring) (explaining that while short-term monitoring is reasonable, long-term monitoring "impinges on expectation of privacy").

179. *Id.* (Alito, J., concurring) (noting that the line into unconstitutionality was crossed before the four-week mark and that police can always seek a warrant if there is any doubt as to the constitutionality of their actions).

180. United States v. Graham, 796 F.3d 332, 341 (4th Cir. 2015); United States v. Davis, 785 F.3d 498, 501 (11th Cir. 2015).

Amendment based off of Justice Alito's concurrence in *Jones*, it is less clear if it is legal to collect any CSLI over shorter periods of time.

There is a need for a bright line rule that holds that any CSLI sought by the police should require a warrant supported by probable cause. While section 2703(d) of the SCA requires only a showing of "specific and articulable facts" that records are relevant to a criminal investigation,[181] the statute should be amended to require a warrant supported by probable cause due to the large quantity of information that can be derived from historical cell site location information. The word "relevant" can be interpreted extremely broad and not necessarily provide the critical level of scrutiny that should be required to access CSLI.[182]

It is true that there is no expectation of privacy in movements on public roads,[183] but the ease with which CSLI can be collected requires a heightened level of scrutiny. Additionally, all of the tracking cases dealt with radio or GPS transmitters in automobiles.[184] While there may be a reduced expectation of privacy in an automobile's movements on a public road,[185] it cannot be extended to a cell phone acting as a tracking device in an individual's pocket or purse. Cell phone tracking is distinguishable from tracking an automobile or an item in an automobile because a cell phone is a de facto extension of the individual as evidenced by its ubiquity in everyday life; although, a GPS tracker is much more accurate than CSLI relying on cell towers to provide location data.[186] The

181. 18 U.S.C. § 2703(d) (2012).

182. *See* Elizabeth Goitein & Faiza Patel, *What Went Wrong With the FISA Court*, BRENNAN CTR. FOR JUSTICE 21–22 (2015), https://www.brennancenter.org/sites/default/files/publications/What_Went_%20Wrong_With_The_FISA_Court.pdf ("In its 2013 decision, the FISA court ruled that all American's phone records were relevant to authorized international terrorism investigations."). In a different context, the use of the word "relevant" in a statute to limit how much information law enforcement can access was circumvented by the government when arguing in front of the Foreign Intelligence Surveillance Court when it sought authorization for the bulk collection of metadata. *Id.*

183. United States v. Knotts, 460 U.S. 276, 281 (1983) (noting that a person traveling in an automobile over public roads has no reasonable expectation of privacy in his or her movements).

184. *See id.* at 278 (beeper in container); *compare* United States v. Karo, 468 U.S. 705, 708 (1984) (beeper in a can), *with United States v. Jones*, 565 U.S. 400, 403 (2012) (GPS on an automobile).

185. *See Knotts*, 460 U.S. at 281 (stating that one generally has a lesser expectation of privacy in cars, and furthermore, that a person driving on a public road has no reasonable expectation of privacy); Rakas v. Illinois, 439 U.S. 128, 153–54 (1978) (distinguishing one's expectation of privacy in cars and other places); South Dakota v. Opperman, 428 U.S. 364, 367–68 (1976) (highlighting the lesser expectation of privacy in cars due to existing government regulations and "public nature of automobile travel"); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (noting the exigency arising from a moving car and lesser expectation of privacy in cars in comparison to a building).

186. Blaze Testimony, *supra* note 26, at 51, 53; *see also* Riley v. California, 134 S. Ct. 2473, 2485 (2014) ("Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.").

Supreme Court in *Kyllo* held that the use of a technological device that is not in common usage by the public to explore details of the home previously unknowable without a physical intrusion constitutes a search under the Fourth Amendment.[187] Just as a thermal imager in *Kyllo* provided the police with information concerning an indoor marijuana growing operation,[188] CSLI can provide the police a clear picture of where a person lives in a manner that is not available to the public.[189]

B. The Need for a Legislative Solution

It is likely that a legislative solution will be necessary to regulate the acquisition of CSLI. In both *Graham* and *Davis* the courts held that despite the unconstitutional collection of CSLI, the police were able to retain the collection of information due to the good faith exception to the exclusionary rule.[190] Law enforcement in each case relied in good faith on an apparently valid court order issued by a neutral magistrate to compel production of CSLI, and in the words of the Eleventh Circuit, law enforcement "acted in scrupulous obedience to a federal statute."[191] With the passage of CalECPA in October 2015,[192] it is possible other states will follow suit. While federal law enforcement will still be able to rely on the SCA for access to CSLI without a warrant, a patchwork of state laws will make law enforcement's work more difficult.[193] A law at the federal level will ensure uniformity among local, state, and federal law enforcement.

Currently, the Court does not appear ready to protect CSLI with a warrant requirement, absent some sort of legislative action. This is quite clear from the *Jones* decision, where the majority applied the tort of trespass to the Fourth

187. Kyllo v. United States, 533 U.S. 27, 40 (2001).

188. *Id.* at 29–30.

189. United States v. Graham, 796 F.3d 332, 349 (4th Cir. 2015) ("Taken together . . . *Kyllo* . . . support[s] our conclusion that the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time. Cell phone tracking through inspection of CSLI is one such technology.").

190. *Id.* at 363; United States v. Davis, 754 F.3d 1205, 1218 (11th Cir. 2014). In *United States v. Leon*, the Court laid out the good faith exception to the exclusionary rule, which states that if police act in good faith on a warrant issued by a neutral magistrate that is subsequently found not to be supported by probable cause, then the evidence obtained by that warrant is not be suppressed because there is no behavior on the part of the police that needs to be deterred. United States v. Leon, 468 U.S. 897, 920–21 (1984).

191. *Davis*, 754 F.3d at 1218 (noting that law enforcement followed the procedures laid out in the Stored Communications Act to access CSLI as reason not to suppress the evidence).

192. *In Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law*, AM. CIVIL LIBERTIES UNION OF N. CAL. (Oct. 8, 2015), https://www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy.

193. Zetter, *supra* note 116.

Amendment to hold the installation of a GPS tracker unconstitutional.[194] Moreover, Justice Alito's concurrence does not provide much support for a warrant requirement for four weeks of tracking without a legislative solution.[195] A warrant requirement is necessary to remedy the serious privacy implications that arise in the collection of CSLI. In the foundational third-party doctrine cases, the defendants took affirmative actions that shared information with third parties.[196]

In the *Davis* and *Graham* cases on the other hand, merely purchasing and carrying a cell phone was enough to grant the government access to months of location data.[197] It may be prudent of the courts to look to the legislature in order to solve the complex privacy issues that arise with cell phones. Sitting *en banc*, the majority echoed this sentiment in *Graham*, emphasizing that while the third-party doctrine controlled in the current case, Congress was free to require greater privacy protections in the form of a warrant requirement for CSLI.[198] Congress should pass a measured piece of legislation that both deals with the current privacy issues arising from the use of CSLI and contains flexibility to ease its adaption to future methods of communication. It is possible that Congress will address the privacy implications of warrantless acquisition of CSLI soon. In 2016, the House of Representatives unanimously passed a warrant requirement for the acquisition of stored email communication.[199] While the legislation languished and ultimately died in the Senate, the broad bipartisan support in the House shows the level of concern about electronic data acquisition that exists among at least one house of Congress. Cell phone use is pervasive in our society, with 72% of respondents in a study stating that they were within five feet of their phones a majority of the time and 12% even admitting that they used their phones in the shower.[200] The *Katz* Court reminds us that the Fourth Amendment

194. United States v. Jones, 565 U.S. 400, 404–05 (2012) ("We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.").

195. *Id.* at 429 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."). While the Supreme Court does not appear ready to weigh in on the CSLI issue, the Fourth Circuit in its Graham decision practically begs the Supreme Court to intervene in the issue. United States v. Graham, 796 F.3d 332, 361 (4th Cir. 2015) ("If the Twenty-First Century Fourth Amendment is to be a shrunken one, as the dissent proposes, we should leave that solemn task to our superiors in the majestic building on First Street and not presume to complete the task ourselves.").

196. *See* Smith v. Maryland, 422 U.S. 735, 741–42 (1979); United States v. Miller, 425 U.S. 435, 440 (1976); United States v. White, 401 U.S. 745, 752 (1971).

197. United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016); United States v. Davis, 785 F.3d 498, 512–13 (11th Cir. 2015).

198. *Graham*, 824 F.3d at 436.

199. Kate Tummarello, *The Fight Over Email Privacy Moves to the Senate*, ELEC. FRONTIER FOUND. (Feb. 7, 2017), https://www.eff.org/deeplinks/2017/02/fight-over-email-privacy-moves-senate.

200. Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM), http://www.cnn.com/2013/07/13/tech/smartphone-use-survey/.

"protects people, not places."[201] A legislatively created warrant requirement for CSLI will accomplish that goal.

IV. CONCLUSION

The courts are legitimately challenged as to how to treat CSLI. Changes in technology always move much faster than the law. As we come to understand how clear a picture of our lives can be discerned solely through accessing CSLI, it is important that the courts provide clear guidance that law enforcement must seek a warrant before accessing historical CSLI. The concurrences in *Jones* show us that the Supreme Court is grappling with the novel privacy issues related to walking around with a device that, while capable of keeping us connected to the world, can also provide significant amounts of information about our private lives. Whether in the courts or in the legislature, it is important for Fourth Amendment jurisprudence to be brought into the twenty-first century by protecting historical location data created by a cell phone that is doing nothing more than traveling in a person's pocket as he or she goes about his business.

201. Katz v. United States, 389 U.S. 347, 351 (1967).