Roger Williams University Law Review

Volume 22
Issue 1 *Vol. 22: No. 1 (Winter 2017)*

Article 8

Winter 2017

Hotline Ping: Harmonizing Contemporary Cell Phone Technology with Traditional Fourth Amendment Protections

Brianne M. Chevalier
Roger Williams University School of Law, Candidate for Juris Doctor, 2017

Comments

Hotline Ping: Harmonizing Contemporary Cell Phone Technology with Traditional Fourth Amendment Protections

Brianne M. Chevalier∗

INTRODUCTION

> "The judiciary must not allow the ubiquity of technology—which threatens to cause greater and greater intrusions into our private lives—to erode our constitutional protections."[1]

A murder has taken place and the police have a suspect who they believe is responsible for the crime. The government wants to place the suspect at the scene of the crime, at the time the crime occurred. Unfortunately, there were no eyewitnesses to identify the suspect, so the government needs an alternative way to prove that its suspect was present at the scene. In order to do so, the government files for a court order that will allow it to

∗ Candidate for *Juris Doctor*, Roger Williams University School of Law, 2017. I am grateful to Professor Emily J. Sack for her wisdom, guidance, and thoughtful suggestions through the entirety of the writing process. Also, to my parents and my sister, thank you for your endless love and support. Lastly, a special thank you to my mom for pushing me to attend law school and for listening to my triumphs and grievances throughout.

1. United States v. Davis, 785 F.3d 498, 533 (11th Cir. 2015) (Martin, J., dissenting).

compel the cell phone service provider to turn over cell site location information from the suspect's cell phone records. This information would include the phone numbers the suspect contacted or was contacted by, as well as the location of the suspect when these connections were made. Should the government be permitted to obtain this type of information from cell service providers (e.g. Verizon, T-Mobile, or Sprint) without a search warrant based on probable cause, and thereby create a play-by-play of a person's location—including, but not limited to, the location where the crime occurred—over a given period of time? Most federal appellate courts have answered this question affirmatively.[2] Under the Fourth Amendment, however, government acquisition of cell phone location records from cell service providers should be considered a search because individuals have a reasonable expectation of privacy in this information.[3] Therefore, obtaining this type of information without a warrant based on probable cause presumably violates the Fourth Amendment.[4]

As technology advances, so too must the application of the Fourth Amendment, specifically with regard to government procurement of cell phone location records from cell service providers. Until May 2016,[5] federal circuit courts were split on the issues of whether (1) obtaining historical cell phone location records from service providers is a "search" under the Fourth Amendment, and (2) if so, whether a "reasonable search" requires the government to obtain a search warrant based on probable cause.[6] Courts face the challenge of determining the legal

2. *See id.* at 500; United States v. Graham (*Graham I*), 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

3. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

4. *See* U.S. CONST. amend. IV ("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.").

5. In May 2016, *Graham* was reheard en banc, overturning the original decision of the Fourth Circuit and thereby abolishing the circuit split that was in place when the case was first decided. United States v. Graham (*Graham II*), 824 F.3d 421, 425–26 (4th Cir. 2016) (en banc). Throughout this Comment, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) will be referred to as "*Graham I*" and United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) will be referred to as "*Graham II*."

6. Megan L. McKeown, Note, *Whose Line is it Anyway? Probable Cause*

standard that law enforcement must meet in order to require the cell service providers to disclose information.[7]

Part I of this Comment will introduce the basic function of cell towers and records, describe the difference between historical and real-time information, and provide a cursory review of the statutory landscape. Part II will discuss relevant Fourth Amendment case law that supplies the framework for determining when there is a search and, if so, when a warrant based on probable cause is required. Part III will focus on the most recent United States Courts of Appeals cases which have occasionally fallen on both sides of the fence regarding the questions of whether a search has occurred and whether a warrant is required. Finally, Part IV will address the strengths and weaknesses of both sides of the arguments. This section will also assert and explain why government acquisition of cell site location information (CSLI) is a search, why a warrant based on probable cause is required, and finally why the Stored Communications Act (SCA), which governs court orders required for attainment of this information, is unconstitutional.

I. CELL PHONE TOWER FUNCTIONS, DATA BASICS, AND APPLICABLE STATUTES

The technologies employed in devices people use every day to work and function in society are often a mystery to those who use such devices. This section explains how the government acquires historical CSLI by connecting to cell towers. Understanding this process is crucial to fully grasp why the government's acquisition of historical CSLI is a search that requires a warrant based on probable cause. Additionally, this explanation is important to understand because the standard for acquisition of this information is currently lower under the SCA than what the warrant requirement entails, and is therefore unconstitutional.

A. *Cell Phone Tower Operations*

Cell phones are supported by a network of cell towers that relay messages from the user, through the service carrier, to the

and Historical Cell Site Data, 90 NOTRE DAME L. REV. 2039, 2039–40 (2015).

7. *See* Peter A. Crusco, *Cell Tower Dumps and the Fourth Amendment*, N.Y.L.J. ONLINE (June 24, 2014).

intended recipient.[8] In 1985, there were just 900 cell phone towers in the United States;[9] however, as of March 2015, the presence of cell towers has increased drastically and there are now over 205,000 throughout the country.[10] These cell towers are placed at various locations throughout a service provider's coverage area.[11] A tower is in constant contact with activated, turned-on cell phones within its proximity so that calls and messages are relayed instantly.[12] The cell phone connects to a cell tower whenever a call or text message is sent or received by the cell phone.[13] The phone will usually connect with, or "ping," the closest cell site where it has the strongest signal.[14] As a cell phone is physically moved to various locations, it "hops" from tower to tower, potentially allowing law enforcement to track the movements of the phone.[15] The accuracy of the location data depends on the size of the geographical coverage range of the cell sites.[16] This Comment exclusively addresses the pinging of cell towers, and not a cell phone's Global Positioning System (GPS) function that is a separate and distinct feature.[17]

Once the nearest cell tower is identified, CSLI can be used to determine the location of the cell phone at the particular point in time that the connection is made.[18] CSLI consists of the dialed digits of calls to and from the telephone number, and the locations and sectors of the cell towers used at the time of the call's origin and termination.[19] Law enforcement officers often use CSLI to

---

8. Leonard Deutchman, *Cell Phone Tracking: Privacy or Anonymity?*, THE LEGAL INTELLIGENCER (Dec. 14, 2010), http://www.ldiscovery.com/law_library/pennsylvania%20law%20weekly%20cell%20tower%20tracking/files/pennsylvania%20law%20weekly%20cell%20tower%20tracking%20.pdf.

9. *Cell Phone Tower Statistics*, STATISTIC BRAIN, http://www.statisticbrain.com/cell-phone-tower-statistics/ (last visited Apr. 3, 2016).

10. *Id.*; Deutchman, *supra* note 8.

11. *Graham I*, 796 F.3d 332, 343 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

12. Deutchman, *supra* note 8.

13. *Graham I*, 796 F.3d at 343.

14. *Id.* Cell site and cell tower are synonymous and will be used interchangeably throughout this Comment.

15. Deutchman, *supra* note 8.

16. *Graham I*, 796 F.3d at 343.

17. To be clear, the pinging of cell phone towers is not something that will soon become obsolete and replaced by the GPS function on a phone. These are two separate and distinct functions of a cell phone.

18. *Graham I*, 796 F.3d at 343.

19. Crusco, *supra* note 7.

develop a list of suspects that were in a crime area at a given time, or to determine that a specific suspect was in an area at the time a crime occurred.[20] Specifically, officers can request that a service provider turn over location data for a suspect over a set period of time—this is called historical CSLI.[21]

There is an important distinction to be made between historical CSLI and real-time information. This Comment will specifically discuss law enforcements' need for a warrant when seeking historical CSLI. Historical CSLI includes records that are already created and maintained by a third-party telephone company[22] and precise data regarding date and time of cell calls, and location of a cell phone.[23] Moreover, the records show incoming and outgoing telephone numbers that connect with the cell tower, including voice calls and text messages.[24] Historical CSLI also includes how long these communications lasted as well as the cell towers used at the beginning and at the end of the communication.[25]

Conversely, real-time data is information collected at the moment in time it occurs.[26] The distinction between these two types of data is important because real-time data raises distinct issues, such as exigency,[27] that historical data does not. To ensure constitutionality, procurement of historical data requires a showing of probable cause, which the SCA does not require.

B. *The Stored Communications Act*

The SCA is the federal statute that governs historical cell site

---

20. *See, e.g.*, United States v. Davis, 785 F.3d 498, 502 (11th Cir. 2015) (Government tracked phone calls to and from defendant's cell phone connected through cell tower locations that were near relevant robbery locations; thus arguing that defendant had to be near robberies as well.).

21. Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-Up*, 110 NW. U.L. REV. 507, 510 (2016).

22. *Davis*, 785 F.3d at 505.

23. *Id.* at 502.

24. Amanda Regan, Note, *Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps*, 43 HOFSTRA L. REV. 1189, 1192 (2015).

25. *Id.*

26. *See* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1748 (2009).

27. *See infra* Part IV.

location information cases.[28] It allows law enforcement to use "'stored user account information compiled by third parties in the ordinary course of business'" without having to prove probable cause.[29] Specifically, the SCA provides:

> A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and 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.[30]

The government can obtain this information by filing for a court order under § 2703(d) requesting information from cell service providers.[31] Court orders differ from search warrants in that the required legal standard to acquire an SCA court order—specific and articulable facts—is much lower than the requirement of probable cause to obtain a search warrant.[32] This lower SCA standard poses a great threat to an individual's Fourth Amendment right; however, while the SCA standard is lower than that for a search warrant, the SCA raised the bar for what is required by the government to obtain information from third

---

28. 18 U.S.C.A. § 2703(d) (Westlaw current through P.L. 114–248); *see, e.g.*, *Graham II*, 824 F.3d 421, 426 (4th Cir. 2016) (en banc); *Graham I*, 796 F.3d 332, 343–44 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); United States v. Davis, 785 F.3d 498, 502 (11th Cir. 2015); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013).

29. Regan, *supra* note 24, at 1196 (quoting Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH & LEE L. REV. 1875, 1896 (2011)).

30. 18 U.S.C.A. § 2703(d) (Westlaw).

31. *See In re Historical Cell Site Data*, 724 F.3d at 615.

32. *Id.* at 606; *see also* 18 U.S.C.A. § 2703(c)–(d) (Westlaw); *In re* United States for an Order Authorizing Release of Historical Cell-site Information, 736 F. Supp. 2d 578, 580 (E.D.N.Y. 2010) (holding that as statutory matter § 2703(c)-(d) permit courts to issue order without showing of probable cause). However, "[s]tatutory authority, of course, is not sufficient if such authority purports to allow, without a showing of probable cause, a search or seizure that must be considered unreasonable under the Fourth Amendment." *Id.* at 581. Thus, "it is manifest that Congress did not purport in enacting that law to definitively accept or reject the reasonableness of any particular expectation of privacy with respect to location tracking—and that therefore the statute is not immune to Fourth Amendment scrutiny." *Id.* at 581 n.9.

parties via a subpoena.[33] For example, "the government routinely issues subpoenas to third parties to produce a wide variety of business records, such as credit card statements, bank statements, hotel bills, purchase orders, and billing invoices."[34] With the enactment of the SCA, Congress demands more information than what is required for a subpoena before the government can retrieve the telephone records from a cell service provider,[35] but, the SCA standard is lower than what is required to obtain a search warrant based on probable cause.[36]

Although the SCA standard is lower than probable cause, it is worth mentioning that it does provide individuals with certain privacy protections.[37] For example, the SCA "generally prohibits telephone companies from voluntarily disclosing such records to a 'governmental entity.'"[38] Among other protections, the SCA provides penalties and remedies for violations of the Act where there was improper disclosure of records.[39] If a judge issues a court order, however, the cell service provider must give out the information requested without being required to provide notice to the customer.[40] The unconstitutionality of the "specific and articulable facts" standard, which is a lower legal standard than that of probable cause, is one of the major concerns regarding the gathering of historical CSLI.[41]

---

33. *See* United States v. Davis, 785 F.3d 498, 505–06 (11th Cir. 2015); *In re Historical Cell Site Data*, 724 F.3d at 606.

34. *Davis*, 785 F.3d at 506; *see, e.g.*, United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985) (motel registration records); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (credit card statements). Additionally, "[t]hose statements not only show location at the time of purchase, but also reveal intimate details of daily life, such as shopping habits, medical visits, and travel plans." *Davis*, 785 F.3d at 506 n.9.

35. *See id.* at 506; 18 U.S.C.A. § 2703(d) (Westlaw).

36. *See* U.S. CONST. amend. IV.

37. *Davis*, 785 F.3d at 506; *see* 18 U.S.C.A. § 2703(d) (Westlaw).

38. *Davis*, 785 F.3d at 506 (citing 18 U.S.C. § 2702(a)(3), (c)(4), c(6)).

39. *Id.* (citing 18 U.S.C. § 2707(a), (c), (d)).

40. *See* Regan, *supra* note 24, at 1197 (citing Elizabeth Elliot, Comment, United States v. Jones*: The (Hopefully Temporary) Derailment of Cell-Site Location Information Protection*, 15 LOY. J. PUB. INT. L. 1, 19 (2013)).

41. 18 U.S.C.A. § 2703(d) (Westlaw).

II. FOURTH AMENDMENT HISTORY AND UNITED STATES COURTS' TAKE ON HISTORICAL CELL SITE DATA

A. *Was There a "Search" Under the Fourth Amendment?*

The Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[42] In analyzing a Fourth Amendment claim, the reviewing court first determines whether or not a search occurred.[43] If there was a search, probable cause and a warrant were required.[44] Then, the reviewing court must determine whether an exception to the warrant requirement applies.[45]

The United States Supreme Court decision in *Katz v. United States* is controlling when analyzing the gathering of historical CSLI because the determination as to whether a "search" has occurred turns on whether a cell phone user has a reasonable expectation of privacy.[46] *Katz* established that the scope of the Fourth Amendment is no longer determined by the absence or presence of a physical intrusion.[47] In a concurring opinion, Justice Harlan advanced a two-part test, which now guides Fourth Amendment analysis to determine whether a search occurred.[48] The first prong of the test focuses on whether the individual had a *subjective* expectation of privacy in the object of the challenged search.[49] If so, the court then analyzes whether society is willing to *objectively* recognize that expectation as reasonable.[50] In order to succeed in claiming that an intrusion was unconstitutional, a party must satisfy both parts of this test.[51] As discussed below,[52]

---

42. U.S. CONST. amend. IV.

43. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 739–40 (1979); Katz v. United States, 389 U.S. 347, 353 (1967); United States v. Robinson, 62 F.3d 1325, 1328 (11th Cir. 1995).

44. *See, e.g.*, *Smith*, 442 U.S. at 745–46; *Katz*, 389 U.S. at 356–57; *Robinson*, 62 F.3d at 1330.

45. *See, e.g.*, *Katz*, 389 U.S. at 357–58.

46. *Id.* at 353. Furthermore, *United States v. Jones* is not applicable here because this is not a situation involving trespass or interference with physical property. *See* 132 S. Ct. 945, 949 (2012).

47. 389 U.S. at 353.

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

49. *Id.*

50. *Id.*

51. United States v. Robinson, 62 F.3d 1325, 1328 (11th Cir. 1995).

52. *See infra* Part IV.

the government's procurement of historical CSLI is a search under the Fourth Amendment and consequently requires a warrant based on probable cause.

B. *The Good-Faith Exception to the Exclusionary Rule*

If a search has occurred, probable cause and a search warrant are required absent an exception. If there is no search warrant and no exception applies, then the Fourth Amendment is violated and the evidence obtained is subject to the exclusionary rule.[53] Exceptions to the warrant requirement include the good-faith exception,[54] which is of particular importance in situations involving warrantless government acquisition of historical CSLI.[55]

The good-faith exception applies when "law enforcement [officers] reasonably rel[y] on (1) an enacted statute, unless that statute is clearly unconstitutional; (2) a search warrant or other court order issued by a neutral magistrate, unless issuance of the order is clearly defective; or (3) binding appellate precedent."[56] For example, the Fourth Circuit originally asserted in *Graham I*[57] that, although the government violated the Fourth Amendment in obtaining historical CSLI without a warrant based on probable cause, the evidence obtained was not suppressed because the government acted in good-faith reliance on court orders issued under the SCA.[58]

As previously mentioned, and more thoroughly discussed below,[59] the standard required for a court order under the SCA is far lower than that for probable cause. This Comment argues that this sub-constitutional standard should not encompass the same good-faith exception. The rights under the Fourth Amendment are protected under the probable cause requirements, but the lowering of constitutional safeguards in the issuance of court orders inevitably mirrors a lowered protection of rights in this

53. Mapp v. Ohio, 367 U.S. 643, 656–57 (1961).

54. United States v. Leon, 468 U.S. 897, 919–22 (1984).

55. *See, e.g.*, *Graham I*, 796 F.3d 332, 362 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

56. *Id.* (citations omitted).

57. *See infra* Part IV. The *Graham II* opinion did not discuss the good-faith exception like the court in *Graham I*; however, the exception must be addressed because it is still a very relevant concern on this topic and may be used in future decisions.

58. *Graham I*, 796 F.3d at 362.

59. *See infra* Part IV.

circumstance, which is unconstitutional.[60] Therefore, the good-faith exception should not apply, as it is not reasonable for the government to rely on such a court order that was not obtained based on the constitutionally required standard.

C. *The Third-Party Doctrine*

Another concept generally applied to searches involving cell phones is the "third-party doctrine," which establishes that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[61] Courts have interpreted the third-party doctrine to support the argument that individual cell phone users assume the risk that information will be disclosed to law enforcement when using their cellular devices.[62] Furthermore, some courts have doubted that "'people in general entertain any actual expectation of privacy in the numbers they dial' because '[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company . . . .'"[63] The third-party doctrine has proven controversial when applied to cell phone location data, however, as many have debated whether this doctrine is still viable in light of the major technological and social changes over the past several decades.[64]

In contrast, some courts have considered the proposition that the doctrine does not apply to cell phone location data because the cell phone user does not voluntarily convey their location information to their service provider.[65] This idea is based on the proposition that "[c]ell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic

60. *See* U.S. CONST. amend. IV.

61. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *accord* McKeown, *supra* note 6, at 2041.

62. *See* United States v. Davis, 785 F.3d 498, 508–09 (11th Cir. 2015) (stressing findings in *Smith* that third-party doctrine can apply to telephone calls to third persons outside of the home); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 612–13 (5th Cir. 2013) (applying *Smith*'s reasoning involving a telephone user to a cell service subscriber).

63. *Davis*, 785 F.3d at 508 (quoting *Smith*, 442 U.S. at 742).

64. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014); Crusco, *supra* note 7, at 2.

65. *Graham I*, 796 F.3d 332, 354 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); Crusco, *supra* note 7, at 2.

participation."[66] This proposition is based on the idea that "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones."[67] Because cell phone users are not voluntarily conveying information to third parties, the third-party doctrine is not applicable; therefore, this information demands Fourth Amendment protection from unreasonable searches.[68]

III. APPLICATION OF THE FOURTH AMENDMENT TO ACQUISITION OF CELL SITE LOCATION INFORMATION

Cell phone records are useful to criminal investigations because they reveal information that shows which cell towers a particular cell phone was closest to in a given period of time—information generally used to place a suspect at a crime scene.[69] Courts disagree on whether or not individuals have a reasonable expectation of privacy regarding their cell phone records or if individuals voluntarily disclose this information through the use of their cell phones.[70] Specifically, there has been disagreement among the courts as to whether it is a search to obtain historical CSLI from service providers, and, if so, whether a warrant based on probable cause is required.[71] These cases do not involve a GPS device, physical trespass, or real-time or prospective cell tower location information.[72] Rather, they narrowly involve only government access to the existing and legitimate business records that a third-party telephone company has already created and maintained, and historical information about which cell tower locations connected the cell phone in question during a given time

66. *Graham I*, 796 F.3d at 355–56.

67. *Id.* at 356.

68. *See* United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring).

69. *See, e.g.*, *Graham I*, 796 F.3d at 341; Deutchman, *supra* note 8.

70. *Compare Graham I*, 796 F.3d at 361 (holding that a person has a reasonable expectation of privacy), *with* United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (holding that no reasonable expectation of privacy because information was voluntarily conveyed to third party).

71. Lance J. Rogers, *Massachusetts Cops Need Warrant for Tower Data*, BLOOMBERG BNA (Sept. 30, 2015), http://www.bna.com/massachusetts-cops-need-n57982059186/.

72. *See Davis*, 785 F.3d at 505.

period.[73]

In *In re United States for Historical Cell Site Data*, the Fifth Circuit held that using the SCA standard—allowing orders that are based on specific and articulable facts—rather than a Fourth Amendment probable cause standard is constitutionally permissible under the Fourth Amendment because people do not have a reasonable expectation of privacy in their cell phone records.[74] The Eleventh Circuit reached a similar conclusion in *United States v. Davis*, holding that no "search" had occurred because the individuals did not possess a reasonable expectation of privacy.[75] The court further held that the SCA standard comports with Fourth Amendment principles and is therefore constitutional.[76]

Conversely, in *Graham I*, the Fourth Circuit held "that the government's procurement and inspection of [the suspects'] historical CSLI was a search, and the government violated [the suspects'] Fourth Amendment rights by engaging in this search without first securing a judicial warrant based on probable cause."[77] The Fourth Circuit has since reversed this decision in *Graham II*.[78]

A. *Is Government Acquisition of Historical CSLI a Search Under the Fourth Amendment?*

1. In re Historical Cell Site Data

In *In re Historical Cell Site Data*, the Fifth Circuit held that no search had occurred because the Fourth Amendment protects only *reasonable* expectations of privacy; therefore, there was no violation of the Fourth Amendment under the third-party doctrine.[79] The court, by employing the two-part *Katz* analysis,

---

73. *See id.*
74. 724 F.3d 600, 615 (5th Cir. 2013).
75. 785 F.3d at 518.
76. *Id.*
77. 796 F.3d at 361.
78. 824 F.3d 421, 424 (11th Cir. 2016) (en banc).
79. 724 F.3d at 615. In this case, the United States filed three applications under § 2703(d) of the . . . SCA, seeking evidence relevant to three separate criminal investigations. Each application requested a court order to compel the cell phone service provider for a particular cell phone to produce sixty days of historical cell site data and other subscriber information for that phone.
Id. at 602 (citations omitted).

determined that no warrant was necessary since there was no reasonable expectation of privacy.[80] In addressing the expectation of privacy, the court explained that "'[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'"[81] Relying heavily on the third-party doctrine, the court agreed with the argument that cell phone users knowingly convey information about their location to their service providers when they make a call and that, even with that knowledge, they voluntarily continue to make such calls foregoing any reasonable expectation of privacy.[82] The court relied on *Smith v. Maryland*, which noted that all subscribers recognize that the phone company controls the equipment that allows their calls to be completed and that the service providers have records for numbers that they dial.[83] The court further explained that even if subscribers do not have this "common knowledge," the government presented evidence that the contract between providers and subscribers expressly stated that a provider both uses and collects a subscriber's location information to route the cell phone calls.[84] Additionally, the court reasoned that the government does not require a member of the public to own or carry a cell phone; rather the use of his or her phone is entirely voluntary.[85]

The court in *In re Historical Cell Site Data* particularly addressed the question of whether the "specific and articulable facts" standard required under the SCA for a court order is constitutional.[86] The court concluded that, by enacting the SCA, Congress crafted a legislative solution to the privacy concerns that develop with advances in technology.[87] The court explained that the SCA is constitutional because cases interpreting the Fourth Amendment,

> [do] not recognize a situation where a conventional order for a third party's voluntarily created business records

80. *See id.* at 608–12.
81. *Id.* at 609 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)) (alteration in original).
82. *Id.* at 612.
83. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 742–43 (1979)).
84. *Id.* at 613 (quoting California v. Greenwood, 486 U.S. 35, 40 (1988)).
85. *Id.*
86. *Id.* at 608.
87. *Id.* at 614.

> transforms into a Fourth Amendment search or seizure when the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from governmental intrusion.[88]

As explained below,[89] the logic employed by this court is flawed considering the relevant and essential role that cell phones have in peoples' lives today, as well as the lack of voluntariness employed by cell phone users.[90]

2. United States v. Davis

Like the Fifth Circuit, the Eleventh Circuit in *United States v. Davis* held that government acquisition of historical CSLI is not a search, and therefore the SCA standard is constitutional under Fourth Amendment principles.[91] Furthermore, the Eleventh Circuit agreed that there is no subjective or objective reasonable expectation of privacy in the historical CSLI records and reiterated the same reasoning provided by the Fifth Circuit.[92] The court explained that "any arguable 'search' should be resolved in favor of the government" in cases such as this because Congress served substantial government interests by enacting the SCA.[93]

The Eleventh Circuit evaluated the SCA standard in a virtually identical way to that of the Fifth Circuit.[94] The court explained that the SCA did not lower the bar for Fourth

---

88. *Id.* at 615. This interpretation protects the reasonable expectations of privacy that the Fourth Amendment recognizes. *Id.* This case is only dealing with the narrow issue of obtaining historical CSLI for specified cell phones via SCA orders. *Id.*

89. *See infra* Part IV.B.

90. Aaron Smith, *Americans and Their Cell Phones*, PEW RESEARCH CENTER (Aug. 15, 2011), http://www.pewinternet.org/2011/08/15/americans-and-their-cell-phones/. As of 2011, 83% of American adults owned some kind of cell phone for the essential tasks of information-seeking and communication. *Id.*

91. 785 F.3d 498, 518 (11th Cir. 2015). In *Davis*, the Government sought to obtain telephone records from the defendant's service provider for a sixty-seven-day period, which was the time span of seven different armed robberies that the police suspected the defendant of committing. *Id.* at 501. The Government's "application requested production of stored 'telephone subscriber records' and 'phone toll records,' including the 'corresponding geographic location data (cell site) . . . .'" *Id.* at 502.

92. *Id.* at 511.

93. *Id.* at 518.

94. *See id.* at 505; *In re* United States for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013).

Amendment purposes, but rather requiring a court order raised the bar from an ordinary subpoena to one with additional privacy protections.[95] As explained in more depth below,[96] the evaluation should not be one that considers how the standard essentially could be worse; the analysis should be strictly focused on whether or not the standard comports with the protections that the Fourth Amendment guarantees.

The Eleventh Circuit attempted to support its reasoning that historical CSLI is very different from GPS data because it does not give as precise of a location as a GPS does.[97] Moreover, while that may be true in certain areas, it is fact-specific based on a cell phone's location.[98] Where more towers exist, and as technology continues to advance, a more accurate location will be obtained.[99] Regardless, the court reasoned that there is no reasonable expectation of privacy in this information and that the information serves a compelling government interest.[100] And, even if individuals are not voluntarily conveying this information and establish a reasonable expectation of privacy in the information, the same information could be obtained and be just as useful to the government's interest if a warrant was required.[101]

3. United States v. Graham I & II

Conversely, the Fourth Circuit, in *Graham I*, decided in 2015 "that the government's procurement of the historical CSLI at issue . . . was an unreasonable search."[102] However, the Fourth Circuit reheard the case en banc in 2016 and reversed the original panel's decision.[103] Nonetheless, the panel decision in *Graham I* provides a thoughtful and thorough analysis, outlining various applicable arguments on the topic. It is also a topic that is likely not yet through running its course in the court system.[104]

---

95. *Davis*, 785 F.3d at 505–06.
96. *See infra* Part IV.D.
97. *Davis*, 785 F.3d at 515.
98. *Id.*
99. *Id.* at 521.
100. *Id.* at 517–18.
101. *See id.* at 518.
102. *Graham I*, 796 F.3d 332, 343 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).
103. *See Graham II*, 824 F.3d 421, 424 (4th Cir. 2016) (en banc).
104. Although *Graham I*, which best supports the thesis of this paper,

After the defendant had been arrested for allegedly committing a series of armed robberies, a detective found two cell phones in the defendant's truck while executing a valid search warrant.[105] Going beyond the scope of that warrant, however, the government sought and obtained court orders for disclosure of historical CSLI for calls and text messages transmitted to and from the cell phones.[106] It then used the court order to obtain historical CSLI from the cell phone service provider for a 221-day time period.[107] Both the circuit panel in *Graham I* and the court in *Graham II* addressed whether the government's acquisition of records without a warrant based on probable cause constituted an unreasonable search in violation of the Fourth Amendment.[108]

In *Graham I*, the circuit panel held that people have a reasonable expectation of privacy in their historical CSLI records and explained 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."[109] The circuit panel reasoned that historical CSLI allows the "government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user."[110] Additionally, applying the third-party doctrine to historical CSLI would essentially permit the government to use a

---

was reheard en banc and overturned, it should be noted that circuit court cases reheard en banc are attractive candidates for review by the Supreme Court. Timothy S. Bishop, Jeffrey W. Sarles & Stephen J. Kane, *Tips on Petitioning for and Opposing Certiorari in the U.S. Supreme Court*, 34 LITIGATION, Winter 2008, at 26, 28. Specifically, one study found that the Supreme Court is three times as likely to grant a petition for certiorari to a case that has been heard en banc as it is to grant certiorari petitions involving panel decisions. *Id.* It is therefore likely that this issue could be heard in the United States Supreme Court and therefore using *Graham I* and its abundance of credible arguments is both necessary and insightful.

105. *Graham I*, 796 F.3d at 340.

106. *Id.* at 341.

107. *Id.*

108. *Id.* at 342.

109. *Id.* at 349.

110. *Id.* at 345. Consider a Massachusetts Supreme Judicial Court decision where the court leaves open the possibility that while generally a search warrant is required, one might not be if the request for historical data is for "a period of six hours or less." Commonwealth v. Estabrook, 38 N.E.3d 231, 237 (Mass. 2015).

person's phone as a tracking device without probable cause.[111] Therefore, *Graham I* determined that the government's acquisition of this information was a search as cell phone users have an objectively reasonable expectation of privacy in this information because of one's expected privacy in private habits and personal activities.[112]

Nevertheless, a circuit split amongst the Fourth, Fifth, and Eleventh Circuits ended when *Graham II* was decided. In *Graham II*, the court held that the government's acquisition of historical CSLI from the defendants' cell phone provider did not violate the Fourth Amendment because United States Supreme Court precedent mandates that the third-party doctrine is controlling in this instance and an individual does not have a reasonable expectation of privacy in historical CSLI.[113] The court explained that the provider only receives the historical CSLI information when a cell phone user's phone exchanges signals with the nearest available cell tower and that it is clear that the user is conveying the information to the service provider.[114] The court also based its holding—that cell phone users voluntarily convey their historical CSLI to service providers—on the proposition that cell phone users understand on some level the basic need to transmit information to the cell service provider in order for the phone to operate properly.[115] The dissenting judge in *Graham II*, although recommending that the defendant's convictions be affirmed under the exclusionary rule's good-faith exception, nevertheless accurately asserted that the Fourth

111. *Graham I*, 796 F.3d at 357.

112. *Id.* at 345.

113. 824 F.3d 421, 424–25 (4th Cir. 2016) (en banc). However, as discussed later in more depth, the Fourth Circuit in *Graham II* seemed to suggest that it is likely that the Supreme Court may very well do away with the third-party doctrine in the future, which would change the outcome of cases involving the government acquisition of historical CSLI. *See id.* at 425.

114. *Id.* at 429. The true issue in this inquiry is not whether the information is being conveyed, but whether it is voluntary. *Id.* at 427.

115. *See id.* at 430. In its reasoning, the court notes that "courts have attached no constitutional significance to the distinction between records of incoming versus outgoing phone calls." *Id.* at 431. However, perhaps as technology advances it will become more apparent that (1) individuals need some form of communicative device such as a cell phone to actively participate in society, and (2) individuals have no control over their phone connecting to a signal when someone calls or messages their phone. Perhaps then may courts begin to make this distinction and realize the lack of voluntariness involved in conveying historical CSLI to service providers.

Circuit "majority's determination that there was no Fourth Amendment violation . . . [is a] conclusion that 'will have profound consequences.'"[116]

B. *If There Was a Search, Is a Warrant Based on Probable Cause Needed to Legitimize the Search?*

Circuit courts are currently in agreement that the government's acquisition of historical CSLI from service providers is not a search and therefore does not require a warrant based on probable cause.[117] The Fourth, Fifth, and Eleventh Circuits have held that no search has occurred because there is not a reasonable expectation of privacy in historical CSLI records, so these courts have not answered the question as to whether a warrant based on probable cause is required to obtain this information. Because the circuit panel declared that there was a reasonable expectation of privacy in this information, and therefore there was a search, the *Graham I* court held that a warrant based on probable cause was required to obtain historical cell site location information.[118] As argued below, when a court does abide by the Fourth Amendment and declares that a search has occurred, the next logical and constitutional step should be to require a warrant based on probable cause because none of the exceptions to the warrant requirement are applicable.[119]

IV. ARGUMENTS IN FAVOR OF AND AGAINST THE GOVERNMENT'S NEED FOR A WARRANT BASED ON PROBABLE CAUSE TO OBTAIN HISTORICAL CSLI DATA

A. *Reasonable Subjective and Objective Expectations of Privacy*

Where a reasonable expectation of privacy exists, government

---

116. *Id.* at 441 n.1 (Wynn, J., dissenting in part and concurring in the judgment) (quoting *Graham I*, 796 F.3d at 378 n.1 (Motz, J., dissenting in part and concurring in the judgment)).

117. The *Graham II* majority recognizes that this issue may very well be reconsidered by the United States Supreme Court in the near future at which time the court could overrule or reject the third-party doctrine and thereby change the format for deciding this issue. *See* 824 F.3d at 425 (en banc).

118. 796 F.3d at 360–61. In *Graham I*, the Court ultimately concluded that the good-faith exception applied and therefore the data obtained was not subject to suppression under the exclusionary rule. *Id.* at 363. However, this panel was overridden on this issue when the case was reheard en banc. *Graham II*, 824 F.3d at 424–25 (en banc).

119. *See infra* Part IV.

procurement of information is a search. In using historical CSLI data to track a cell phone's location, the government uses technology not available to the general public.[120] Additionally, some courts have put a great emphasis on the extended amount of time that the government monitors when obtaining the historical CSLI, suggesting that perhaps a short amount of time would not require a warrant, but a longer amount could.[121] However, while the increased amount of time and information gathered is certainly concerning, if an individual has a reasonable expectation of privacy in their historical CSLI, requiring a warrant should not hinge on an amount of time. Making a warrant requirement based on a vague standard will only create more ambiguity in future situations.

Society's reasonable expectation of privacy has changed as technology has advanced.[122] One school of thought asserts that "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[123] However, this argument is groundless. An individual should not be forced to exchange his or her constitutional right to be free from unreasonable searches for innovations in and use of technology. The Fourth Circuit eloquently articulated this point in *Graham I* when it asserted that "the advent of new technology alone—even major technological advances—is not a sufficient basis upon which to infer an equally dramatic shift in people's privacy expectations."[124]

---

120. *See Graham I*, 796 F.3d at 349 ("The Government invades a [person's] 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." (emphasis added)).

121. *See, e.g.*, Commonwealth v. Estabrook, 38 N.E.3d 231, 238 (Mass. 2015).

122. *See In re* United States for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013). For example, consider how several years ago individuals could travel through an airport and board an airplane without passing through a metal detector, taking their shoes off, taking certain items out of their bags, having their bags screened, or possibly being stopped for further examination. Today, however, technology has existed long enough to consider these procedures as normal and routine. Thus, over time an individual's expectation of privacy in his or her belongings has been greatly reduced.

123. *Id.* (quoting United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012)).

124. 796 F.3d at 359.

Additionally, the abundance of information revealed through historical CSLI strongly suggests that there is a reasonable expectation of privacy in the records. In *In re Historical Cell Site Data*, the defense devoted part of its argument "on what information cell site data reveals—location information" to prove the unconstitutionality of the SCA standard.[125] It also analyzed the government's request for the historical CSLI under the framework of United States Supreme Court precedents on tracking devices.[126] Obtaining historical CSLI and gaining information from tracking devices are similar in that both produce location data of an individual for a given amount of time, and both may track individuals to their home; a place that generally has been given heightened protections by the courts. Distinct differences between the two location-gathering strategies, however, make it even more reasonable that historical CSLI would be protected under the Fourth Amendment against a warrantless search, just like the prolonged GPS monitoring of a vehicle.[127]

The defense also indicated that cell phones can travel places that cars or containers cannot go or are unlikely to go, which makes tracking historical CSLI more intrusive than GPS monitoring.[128] For example, while a car may take someone from one location to another, they could easily get in another vehicle, take public transportation, or go to an area that may not be accessible by a car. While a GPS is obviously intrusive, historical CSLI can reveal just as much, and more, about a person's movements.

Another common, yet defective, argument against requiring the government to obtain a warrant before acquisition of historical CSLI is that the information obtained is much less intrusive than using a GPS to monitor a person's movements or examining the content of an individual's cell phone. This argument, however, does not take into consideration the amount of information that can be discovered from a historical evaluation of an individual's CSLI. Justice Sotomayor persuasively exhibited this in her concurrence in *United States v. Jones*, when she described what is

125. 724 F.3d at 608.
126. *Id.*
127. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012).
128. *In re Historical Cell Site Data*, 724 F.3d at 609.

known as the "Mosaic Theory."[129] She posits, "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."[130] As technology advances and more cell towers are constructed, the precision of the location that historical CSLI will be able to provide to the government will essentially paint a picture of an individual's life. It is undeniable that this type of surveillance of an individual is neither subjectively nor objectively reasonable.

B. *The Third-Party Doctrine Is "Ill Suited to the Digital Age"*[131]

Parties have taken several different approaches in arguing about whether the government needs a warrant based on probable cause to obtain historical CSLI from cell service providers. For example, in *In re Historical Cell Site Data*, the government argued that cell phone users voluntarily convey their location to their service providers when they make a call and that they nonetheless voluntarily continue to make such calls.[132] In opposition, the ACLU contended that a cell phone user is not voluntarily conveying his location because "[w]hen a cell phone user makes or receives a call, there is no indication to the user that making or receiving that call will . . . locate the caller" and therefore a user cannot voluntarily convey something he does not know he has.[133] The court declared that cell phone users do voluntarily convey their information because they understand that their cell phones must send a signal to a nearby tower in order to connect a call.[134]

Absent clear reasoning, the Fifth Circuit agreed with the government's argument that the conveyance of information is voluntary.[135] The court asserted that the cell phone user is sending the information so that the provider can perform the

129. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
130. *Id.* (Sotomayor, J., concurring).
131. "Justice Sotomayor has suggested 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.'" *Graham II*, 824 F.3d 421, 438 (4th Cir. 2016) (en banc) (quoting *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring)).
132. 724 F.3d at 612.
133. *Id.* (alteration in original).
134. *Id.* at 613.
135. *Id.*

service of connecting calls made to other users.[136] Nonetheless, it is very important to note that cell towers are pinged when cell phone users make calls or send text messages, as well as when they receive calls and messages.[137] Therefore, the cell user is not technically conveying the information to the cell providers themselves simply by possessing a phone and a cell phone user is certainly not voluntarily turning over this information. It is not constitutionally sound to "force an ill-fitting presumption of voluntariness in order to strip Fourth Amendment protection from a defendant."[138]

The Fourth Circuit correctly held in *Graham I* that it was clear that cell phone users do not voluntarily convey historical CSLI to service providers.[139] The *Graham I* opinion explained that individuals are not conveying this information to service providers; rather the service provider automatically generates this information, both "with and without the user's active participation."[140] Furthermore, the *Graham I* court made an important distinction between historical CSLI records and the records that were involved in *Smith* and *Miller*, explaining that unlike phone numbers dialed or bank records created, respectively, historical CSLI is neither tangible nor visible to a cell phone user.[141] Common sense would lead one to believe that something so intangible that an individual does not have the option but to technically "convey" would not be subject to the third-party doctrine as it is clearly not voluntary.

A cell phone user's knowledge about how the cell signals and towers work is not what is at issue in this particular argument.[142] Rather, the issue is whether the information is being conveyed to the service providers voluntarily. For instance, many individuals are aware that the government is capable of listening to phone

136. *Id.*
137. *See Graham I*, 796 F.3d 332, 355 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).
138. *Graham II*, 824 F.3d 421, 443 n.3 (4th Cir. 2016) (en banc) (Wynn, J., dissenting).
139. *Graham I*, 796 F.3d at 353.
140. *Id.* at 354.
141. *Id.* at 355.
142. *See Graham II*, 824 F.3d at 445 (en banc) (Wynn, J., dissenting) ("[E]ven if cell phone customers have a vague awareness that their location affects the number of 'bars' on their phone, they surely do not know which cell phone tower their call will be routed through . . . ." (citation omitted)).

conversations, but that does not mean that individuals do not have a reasonable expectation of privacy in those conversations. On the contrary, the term "voluntary" and what constitutes as a voluntary conveyance is the major point of discrepancy in determining whether cell phone users have a reasonable expectation of privacy in their historical CSLI. If cell phone users truly convey their location voluntarily to cell service providers, they would not have a reasonable expectation of privacy, and consequently there would be no search and no warrant requirement. However, individuals cannot expect to have voluntarily conveyed information via a device that is crucial to active participation in today's society.[143]

Moreover, this argument is strongly supported by statistics of both the percentage of Americans who own cell phones, as well as the percentage of Americans living in households with only wireless telephone service. About ninety-seven percent of adults had a cell phone in 2013, whereas about forty-seven percent of households have only wireless telephone service in 2016.[144] The high percentage of adults who possess cell phones proves that, for better or for worse, these devices have become an integral part of life.[145] It is at odds with common sense to conclude that a person voluntarily conveys information through a mechanism that requires them to do so in order to function as a member of society. Once a person's choice becomes so drastic that it is between participation in society or protecting their Fourth Amendment right, the choice is no longer voluntary. The third-party doctrine is employed to restrict Fourth Amendment protections to situations where privacy claims are reasonable, not to diminish Fourth Amendment protections where developing technology

143. *See Graham I*, 796 F.3d at 355–56 (citing Riley v. California, 134 S. Ct. 2473, 2484 (2014); City of Ontario v. Quon, 560 U.S. 746, 760 (2010)).

144. Maranda Gibson, *Cell Phone Statistics: Updated 2013*, ARKADIN COLLABORATION SERVICES (Jan. 23, 2014), https://www.accuconference.com/blog/cell-phone-statistics-updated-2013/; Kyley McGeeney, *Pew Research Center will call 75% Cellphones for Surveys in 2016*, PEW RESEARCH CENTER (Jan. 5, 2016), http://www.pewresearch.org/fact-tank/2016/01/05/pew-research-center-will-call-75-cellphones-for-surveys-in-2016/.

145. In addition to communication, cell phones are important because they save people money. *Importance of Mobile Phone Technology*, MY ESSAY POINT (Feb. 1, 2015), http://myessaypoint.com/importance-of-mobile-phone-technology. They are an all-in-one device, thus helping businesses function more efficiently, as well as ensuring personal safety. *Id.*

provides new ways to obtain private information.[146] Since cell phone users do not voluntarily convey historical CSLI to service providers, "the third-party doctrine alone cannot resolve whether the government . . . conducted a Fourth Amendment 'search.'"[147] Rather, an independent Fourth Amendment evaluation is needed to determine whether "the government violates a subjective expectation of privacy that society recognizes as reasonable" by obtaining historical CSLI.[148]

Importantly, while the court in *Graham II* did reverse the decision in *Graham I*, the court explicitly stated that "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine."[149] The court also stated that "unless and until the Supreme Court holds, [it is] bound by the contours of the third-party doctrine . . . ."[150] It is not unreasonable to assume based on the language of the Fourth Circuit and its multiple references to the day that the United States Supreme Court eliminates the third-party doctrine, that the court in *Graham II* chose to include that language to acknowledge the obvious shortcomings of the third-party doctrine. Additionally, the Fourth Circuit likely used this language to suggest that if the United States Supreme Court did make the decision to do away with the doctrine that it would not be considered irrational. Moreover, it could also be inferred from this statement that the court would have come to a different conclusion on whether an individual has a reasonable expectation of privacy in historical CSLI if the third-party doctrine were not controlling precedent.

C. *Historical CSLI is Only Available Through Technological Means*

The Fourth Circuit persuasively stated: "The Supreme Court has recognized an individual's privacy interests in comprehensive accounts of her movements, in her location, and in the location of her personal property in private spaces, particularly when such information is available only through technological means not in

146. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 527 (2011).
147. *Graham II*, 824 F.3d at 446 (en banc) (Wynn, J., dissenting).
148. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).
149. *Id.* at 425 (majority opinion).
150. *Id.* at 437.

use by the general public."[151] This argument has great weight here. Historical CSLI allows the government to place an individual in a variety of places, including private places such as the home.[152] This type of search should be granted a great deal of protection because like *United States v. Karo*[153] and *Kyllo v. United States*,[154] it has the effect of placing the government in an individual's home. Moreover, the Fourth Circuit correctly points to the fact that inspection of long-term historical CSLI gives rise to an even greater privacy interest than in *Karo* and *Kyllo* because a cell phone is carried by a person, can go places that other devices are not likely to go, and thus can directly track an individual.[155]

D. *The SCA Standard is Unconstitutional*

First and foremost, since government acquisition of historical CSLI is a search, the SCA standard of specific and articulable facts is unconstitutional. The SCA standard allows the government to conduct searches without having to show probable cause, contrary to Fourth Amendment jurisprudence. Both the Fifth and Eleventh Circuit courts have evaluated the SCA standard by considering the added protections that Congress instated with the SCA that did not exist prior to its enactment when all that was needed was a subpoena.[156] The proper analysis, however, is not how far the standard has developed, but whether or not the standard is in compliance with Fourth Amendment principles.

This analysis seems inconsistent because the courts are essentially saying, "The government is doing better than they used to," but that is not enough when a person's fundamental

151. *Graham I*, 796 F.3d 332, 345, *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016) (4th Cir. 2015).

152. *See id.* at 346.

153. 468 U.S. 705, 714 (1984) (holding that government's "monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.").

154. 533 U.S. 27, 40 (2001) (holding that government's use of a device not available to general public to explore details of home that would previously have been unknowable without physical intrusion violates the Fourth Amendment).

155. *Graham I*, 796 F.3d at 347.

156. United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 607 (5th Cir. 2013).

right to be free from unreasonable searches and seizures is at stake. This right has a long-standing history of protection throughout Fourth Amendment jurisprudence and advancements in technology should not skew the courts' analyses. Additionally, even if these records could be analogized with other types of records that the government acquires with a subpoena, here, these records can be distinguished because the information that comprises the historical CSLI is not being voluntarily conveyed to the service provider.

E. *Rebutting Argument that Requiring a Warrant Allows Criminals to Circumvent the System and Why the Lack of Applicability of the Exigency Exception Undermines This Argument*

In focusing on the acquisition of historical CSLI, it is unclear how requiring the government to obtain a warrant before procuring historical CSLI from cell service providers would allow criminals to outwit the justice system.[157] Unlike other forms of evidence that could be destroyed if not obtained quickly, the data involved in these searches is historical and already stored by the service providers. Consequently, unless in the unlikely event that a criminal has an inside connection with a service provider who can erase this information before the government can obtain a warrant, this argument is null. Therefore, an exigency argument cannot support the assertion that law enforcement tactics must be allowed to advance with technology. Because the data in question is all historical data, time is not of the essence.[158] Rather, the data is already collected and getting a warrant within a reasonable amount of time would not affect the information. Regardless of the amount of time that a service provider maintains the historical CSLI, due to the relatively short amount of time that it takes to obtain a warrant in today's court systems, it would not make a great difference in the government's ability to secure the data before it was destroyed.

In *Davis*, the Eleventh Circuit asserted that allowing the government to obtain historical CSLI without a warrant assists in

157. *See In re Historical Cell Site Data*, 724 F.3d at 614 (quoting United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012)).

158. The argument that time is not of the essence for historical CSLI assumes that the service provider maintains the records for a reasonable amount of time.

investigations, particularly in the early stages "when the police lack probable cause and are confronted with multiple suspects."[159] The court further stated that the SCA court order allows the police to "help . . . build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources."[160] While this may be accurate, the ease of police work cannot be a justification for limiting an individual's Fourth Amendment protection against unreasonable searches. There are likely several instances where allowing the police to circumvent the warrant requirement would be beneficial to an investigation, but that is not a reason to take away a constitutional protection. The Eleventh Circuit also asserted the government's compelling interest in ensuring that the rights of innocent suspects are vindicated.[161] However, whether an individual is innocent or guilty, his or her constitutional rights should remain intact.

F. *The Amount of Time and Resources to Obtain a Warrant Is an Invalid Argument*

It is not a waste of time or resources to require the government to obtain a warrant every time it wishes to obtain historical CSLI. A judge issuing a court order still has to check if the SCA's specific and articulable facts standard is met, just as a judge has to consider if the probable cause standard has been met to obtain a warrant.[162] Furthermore, law enforcement is still going to court and using essentially the same resources to obtain a court order as when they obtain a warrant. Particularly, for historical CSLI, there is no rush for this information because it is not real-time, and it is not likely to be destroyed in the amount of time that it would require to get a warrant. Allowing the government to procure this type of information without a warrant is allowing the police, not criminals, to circumvent the criminal justice system.

---

159. *Davis*, 785 F.3d at 518.
160. *Id.*
161. *Id.*
162. *See, e.g.*, *Google Transparency Report*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/legalprocess/#whats_the_difference (last visited Sept. 25, 2016).

G. *Looking Forward to Further Advancements in Technology*

The precision of the historical CSLI in these cases is dependent on the size of the coverage ranges of the cell sites.[163] In urban areas, where there is a greater density of cell towers with smaller radii of operability, there is better accuracy of location.[164] In *Graham I*, the court explained that "[s]ervice providers have begun to increase network capacity and to fill gaps in network coverage by installing low-power cells such as 'microcells' and 'femtocells,' which cover areas as small as 40 feet."[165] As companies compete, it is only natural that this technology will continue to advance and become more capable of extremely precise location.[166]

With more precision, historical CSLI further infringes on an individual's Fourth Amendment protection by providing a more discrete location than it currently does. As technology advances and cell phones become an even more intricate part of a person's everyday life, cell towers will either increase in number or become better at locating the individual. The existing competition between cell service providers can be seen in the various commercials and advertisements that cell service providers use today, arguing with each other over who has the fastest connection, a trait that is based on a tower's presence or absence in a given area.[167]

---

163. *See Graham I*, 796 F.3d 332, 343 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016). For example, as seen in that case, "Sprint/Nextel's custodian testified at trial that the cell sites listed in the records each had, at most, a two-mile radius of operability. Each cell site, therefore, covered no greater than approximately 12.6 square miles, divided into three sectors of approximately 4.2 square miles or less." *Id.* at 350 n.9.

164. *See id.* at 343.

165. *Id.* at 350–51 (citing *Public Safety Tech Topic #23–Femtocells*, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/help/public-safety-tech-topic-23-femtocells (last visited Sept. 25, 2016); *Small Cells Market 2014-2019: Femtocell, Picocell, & Microcell Prospects for LTE, SONs, Wireless Offloading & Heterogeneous Networks*, PR NEWSWIRE (Apr. 7, 2015 8:10 AM), http://www.prnewswire.com/news-releases/small-cells-market-2014-2019-femtocell-picocell-microcell-prospects-for-lte-sons-wireless-offloading-heterogeneous-networks-300061444.html; Nancy Gohring, *Femtocells Make Way into Enterprises*, COMPUTERWORLD (Mar. 7, 2011 6:00 AM), http://www.computerworld.com/article/2550032/mobile-wireless/femtocells-make-way-into-enterprises.html).

166. *See id.* at 351.

167. *See, e.g.*, Alex Wagner, *T-Mobile Uses Colorful Balls to Compare its LTE Coverage to Verizon's in New Ad*, TMONEWS (Jan. 24, 2016),

Often, courts will defer to the legislature to make a change or decision that they believe that branch of the government is more suited to make.[168] While the legislature may be able to resolve this case by abolishing the SCA standard, the court is also capable of addressing this issue, mostly because the standard is in direct contradiction with a constitutional right. There are several valid arguments in support of holding the SCA standard unconstitutional, and it would not be contrary to Fourth Amendment precedent for the court to hold so.

CONCLUSION

The Fourth Amendment not only "permit[s] access to that which technology hides" but also "protect[s] that which technology exposes."[169] Individuals have a reasonable expectation of privacy in historical CSLI data. Moreover, individuals are not voluntarily conveying this information to service providers. Conveyance of historical CSLI is "'not voluntary,' for '[l]iving off the grid . . . is not a prerequisite to enjoying the protection of the Fourth Amendment.'"[170] Because individuals have a reasonable expectation of privacy in this information, the acquisition of this information is a search. Under the Fourth Amendment, this type of search requires a warrant based on probable cause. If an individual's constitutional rights are to be upheld on this issue, the United States Supreme Court would abolish the third-party doctrine as it applies to historical CSLI and create a standard whereby individuals are not faced with the choice of using technology and participating actively in society or their guaranteed constitutional protection under the Fourth Amendment.

---

http://www.tmonews.com/2016/01/t-mobile-uses-colorful-balls-to-compare-its-lte-coverage-to-verizons-in-new-ad/; Adrian Diaconescu, *T-Mobile and Sprint Bust Verizon's Balls . . . Ad with Comical New Commercials of Their Own*, POCKETNOW (Jan. 25, 2016, 6:25 AM), http://pocketnow.com/2016/01/25/t-mobile-sprint-verizon-balls-commercials.

168. *See* United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

169. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009).

170. *Graham II*, 824 F.3d 421, 433 (4th Cir. 2016) (en banc) (alteration in original).