BIG BROTHER IS WATCHING YOU: GOVERNMENT SURVEILLANCE THROUGH CELL-SITE LOCATION INFORMATION AND THE FOURTH CIRCUIT'S ATTEMPT TO STOP IT

INTRODUCTION

The Fourth Amendment to the United States Constitution has long protected the people of the United States from unreasonable searches and seizures.[1] However, this protection does not extend to all searches and seizures, only to those that are deemed unreasonable under the law.[2] The Supreme Court has traditionally considered warrantless searches presumptively unreasonable.[3] The present digital age has made the application of the Fourth Amendment increasingly problematic, as the judiciary is constantly called upon to redefine what is and is not reasonable.[4] Most recently, the judiciary has been called upon to determine whether the warrantless procurement of cell-site location information ("CSLI") violates the protections of the Fourth Amendment.[5]

Most courts—specifically the Third, Fifth, and Eleventh Circuits—have concluded that the warrantless procurement of CSLI is not per se unconstitutional.[6] On August 5, 2015, in *United States v. Graham*,[7] the Fourth Circuit broke away from its sister circuits and held that the warrantless procurement of CSLI is unconstitutional.[8] However, since the publication of this Note, the Fourth Circuit vacated this decision pending a rehearing en banc, tentatively scheduled for oral argument during the court's March 22–25, 2016, oral argument session.[9] This Note argues that the full Fourth Circuit should uphold the three-judge panel's decision in

---

1. *See* U.S. CONST. amend. IV.
2. *E.g.*, Boyd v. United States, 116 U.S. 616, 641 (1886).
3. Kentucky v. King, 553 U.S. 452, 459 (2011); *see also* Megan L. McKeown, Note, *Whose Line Is it Anyway? Probable Cause and Historical Cell Site Data*, 90 NOTRE DAME L. REV. 2039, 2039 (2015) (discussing warrantless searches to obtain a cell phone's location information).
4. Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/.
5. *See* United States v. Graham, 796 F.3d 332, 338 (4th Cir.), *reh'g granted*, 624 F. App'x 75 (4th Cir. 2015) (mem.).
6. *See infra* Part IV. A–C.
7. 796 F.3d 332 (4th Cir. 2015).
8. *Id.* at 338.
9. United States v. Graham, 624 F. App'x 75, 75 (4th Cir. 2015) (mem.).

Graham and conclude that the warrantless procurement of CSLI is unconstitutional.

Part I of this Note orients the reader to the technology and law at issue—specifically, CSLI technology, the Fourth Amendment, and the Stored Communications Act. Part II addresses the facts and procedural history of *Graham*, while Part III discusses the 2–1 majority decision in *Graham*. Part IV notes how other federal circuit courts—particularly, the Third, Fifth, and Eleventh Circuits—district courts, and state supreme courts have addressed the collection of CSLI. Part V argues that, under the *Katz v. United States*[10] analysis, the warrantless procurement of CSLI violates the Fourth Amendment and the third-party doctrine is inapplicable to the collection of CSLI. Finally, this Note concludes by urging the Fourth Circuit, and the Supreme Court for that matter, to similarly conclude that the warrantless procurement of CSLI is unconstitutional.

I. BACKGROUND

A. *Cell-Site Location Information Technology*

In order to understand how the Fourth Amendment is implicated regarding CSLI technology, it is important to understand what this technology is, how it is collected, and what kind of information it provides government authorities. Thus, to begin, CSLI refers to "cell-site location information."[11] Cell phone service providers furnish service towers that communicate with its users' cell phones.[12] Cell phones constantly communicate with these service towers through a process called "registration."[13] Registration does not require any action by the user, and it even occurs without the user's knowledge.[14] Unless the cell phone is turned off, it will continuously register with service towers every seven seconds.[15]

As the user moves from one service tower toward a second service tower, the signal strength at the first tower will inevitably decrease while the signal strength at the second tower will increase.[16] Consequently, the cell phone must reregister with the

10. 389 U.S. 438 (1928).
11. Meyer, *supra* note 4.
12. 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, 1747 (2009).
13. Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).
14. *Id.*
15. *Id.*
16. *Id.*

second tower in order to provide the strongest possible signal.[17] However, what happens if the user is walking in an area that provides comparative signal strengths from two or more towers? In other words, what happens when a cell phone is receiving signals of equal strength from multiple service towers?

When this happens, service providers employ more precise location methods to determine which service tower the cell phone should reregister with.[18] The two most common methods are Time Difference of Arrival ("TDOA") and Angle of Arrival ("AOA").[19] Through TDOA the service provider estimates the distance between the service tower and the phone by measuring the amount of time it takes for a signal to travel between the user's cell phone and the service tower.[20] In contrast, AOA determines a cell phone's "location based on the angle at which its signal reaches the tower."[21] These location methods become even more precise when three service towers are involved, as it permits service providers to triangulate the user's precise location.[22]

How precise of a location these data provide depends on various factors, including whether the user is in a rural or urban area.[23] In a rural area, service towers may be miles apart, and thus, there is significantly less detail regarding the user's location.[24] In contrast, service towers have become increasingly concentrated in urban areas.[25] Therefore, service providers can estimate a user's location within a couple hundred feet.[26] From there, the user's location can be narrowed even further. For instance, service towers are divided into three, 120-degree "faces."[27] Service providers can determine which direction a user is located based upon which "face" receives the cell phone's signal.[28] Furthermore, as previously noted, when three towers are involved, service providers can triangulate the precise location of the user.[29]

The advent of the smartphone has brought about additional problems regarding the collection of CSLI. Today, over ninety percent of cell phones contain built-in global positioning system

---

17. Chamberlain, *supra* note 12, at 1753.
18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 710 (2011).
24. McLaughlin, *supra* note 13, at 426–27.
25. Chamberlain, *supra* note 12, at 1754.
26. McLaughlin, *supra* note 13, at 426.
27. Chamberlain, *supra* note 12, at 1754.
28. *Id.*
29. *Id.*

("GPS") location tracking capabilities.[30] Although it is unclear whether GPS data is included in the collection of CSLI, GPS technology provides even more precise location movements.[31] Furthermore, smartphones are often in constant operation.[32] Thus, a smartphone not only registers with a service tower every seven seconds, but also every time a call is placed or received, a text message is sent or received, e-mail is refreshed, or a background application is updated, among other user activities.[33]

B. Fourth Amendment Jurisprudence

The Fourth Amendment to the US Constitution guarantees:

> 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.[34]

Traditionally, the Supreme Court analyzed "unreasonable searches and seizures" under common law trespass.[35] In *Katz* the Supreme Court diverged from this exclusive property-based approach and held that a search occurs when: (1) a person exhibits "an actual (subjective) expectation of privacy" and (2) that expectation is one society deems reasonable.[36]

Since the *Katz* analysis emerged, the continuous evolution of technology has required courts to address numerous investigative technologies, often on a technology-by-technology basis.[37] Recently, in *United States v. Jones*,[38] the Supreme Court addressed whether the installation of a GPS tracking device in an individual's vehicle to monitor his movements constituted a search under the Fourth Amendment.[39] While the Supreme Court relied on the traditional trespass theory to hold that such methods constitute a search, the Supreme Court reaffirmed the application of the *Katz* analysis to the transmission of electronic signals.[40] Furthermore, the Supreme

---

30. McLaughlin, *supra* note 13, at 427.
31. *See* McKeown, *supra* note 3, at 2051 n.93; McLaughlin, *supra* note 13, at 427.
32. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014).
33. Freiwald, *supra* note 23, at 703, 707.
34. U.S. CONST. amend. IV.
35. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464–66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967); *see also* McKeown, *supra* note 3, at 2043–45 (discussing early Fourth Amendment jurisprudence).
36. Katz v. United States, 389 U.S. 347, 361 (1967).
37. McLaughlin, *supra* note 13, at 429.
38. 132 S. Ct. 945 (2012).
39. *Id.* at 948.
40. *Id.* at 953.

Court expressed concern regarding the traditional application of Fourth Amendment jurisprudence in the current digital age, particularly as it relates to cell phone technology.[41] This concern was further expressed in *Riley v. California*,[42] in which the Supreme Court held that a warrant is required in order to search the contents of an individual's cell phone.[43] Once again, the Supreme Court reemphasized its concern that the traditional approach of Fourth Amendment jurisprudence may be outdated for the current digital age.[44] Nevertheless, the Supreme Court has yet to affirmatively address the constitutionality of the warrantless procurement of CSLI under the Stored Communications Act.

C. *The Stored Communications Act*

The Stored Communications Act ("SCA") falls under Title II of the Electronic Communications Privacy Act of 1986.[45] The SCA "regulates the disclosure of stored wire and electronic communications information."[46] Communications information sought by the government is divided into the following "two mutually exclusive categories:" (1) the content of communication; and (2) other records or information regarding a customer's electronic communication (excluding content).[47] Compelled disclosure for information under the second category is governed by section 2703(c) of the SCA.[48] CSLI (arguably) falls into this category.[49]

Section 2703(c) permits the government to compel disclosure via three general methods: (1) a warrant; (2) the consent of the customer; or (3) a court order under section 2703(d).[50] In relevant portions, section 2703(d) provides:

> 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

41. *See id.* at 954–57 (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring).
42. 134 S. Ct. 2473 (2014).
43. *Id.* at 2493.
44. *See id.* at 2489–92.
45. 18 U.S.C. §§ 2701–2712 (2012); Chamberlain, *supra* note 12, at 1755.
46. Chamberlain, *supra* note 12, at 1755.
47. *Id.* at 1756.
48. *See* 18 U.S.C. § 2703(c).
49. *See* Chamberlain, *supra* note 12, at 1757–58 (noting how opponents to this categorization argue that cell-site location information ("CSLI") falls within the "tracking device" exception under the SCA).
50. 18 U.S.C. § 2703(c)(1).

> or other information sought, are relevant and material to an ongoing criminal investigation.[51]

This "specific and articulable facts" standard is significantly less stringent than the warrant requirement of probable cause.[52] Therefore, the government consistently relies on section 2703(d) to compel disclosure of CSLI.[53] However, as we will see, the current digital age has made such reliance increasingly problematic.

II. FACTS AND PROCEDURAL HISTORY TO *UNITED STATES V. GRAHAM*

A. Facts

On the afternoon of February 5, 2011, a Burger King and a McDonald's were robbed in Baltimore City, Maryland.[54] Witnesses to the robberies provided officers a description of the robbers and the getaway vehicle.[55] Ten minutes after the McDonald's robbery, two individuals, later identified as Aaron Graham and Eric Jordan (the "defendants"), were apprehended.[56] Officers recovered a handgun, money, and two cell phones that belonged to the defendants.[57]

Initially, the defendants were only charged with firearm violations.[58] At the time, however, there was an ongoing investigation into several other Baltimore area robberies.[59] Thus, pursuant to the SCA, the government applied for an order that Sprint/Nextel disclose the identification and address of cell-site locations related to the use of the defendants' cell phones.[60] Despite the fact that the defendants were charged with neither the February 5 robberies nor any other robberies in the area, the government sought CSLI for the following four periods: August 10–15, 2010; September 18–20, 2010; January 21–23, 2011; and February 4–5, 2011 (the "First Order").[61] The government sought this data in order to "conclusively link" the defendants to the February 5 robberies, as well as several other robberies that occurred in the area.[62]

---

51. *Id.* § 2703(d).
52. Chamberlain, *supra* note 12, at 1757.
53. *See, e.g.*, *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006) (using the section 2703(d) standard to permit the disclosure of CSLI).
54. United States v. Graham, 846 F. Supp. 2d 384, 385–86 (D. Md. 2012).
55. *Id.* at 386.
56. *Id.*
57. *Id.* The two cell phones, a blue Samsung and a silver Sanyo, belonged to Aaron Graham and Eric Jordan, respectively. *Id.*
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*

To obtain an order requiring a cell phone service provider to disclose CSLI, Section 2703(d) of the SCA requires that the government provide "specific and articulable facts showing that there are reasonable grounds to believe that the [data is] relevant and material to an ongoing criminal investigation."[63] The magistrate judge concluded that the government met this standard and thus granted the government's First Order.[64] Consequently, the government amended the defendants' original indictment to include the February 5 robberies.[65]

After this indictment, the government received new information regarding additional related robberies in the Baltimore County area.[66] The government presented this information to a grand jury, which returned a "Second Superseding Indictment" against the defendants to include these robberies.[67] However, because the government failed to include the relevant time periods for these robberies in its initial application for CSLI, the government filed for a second application for CSLI from July 1, 2010, through February 6, 2011 (the "Second Order").[68] The magistrate judge concluded that the government met the requisite standard and thus similarly granted the Second Order.[69] Sprint/Nextel complied with both Orders and provided the government with the relevant data.[70] At pretrial, the defendants filed a motion to suppress the CSLI obtained by the government.[71] The district court's opinion thus followed.

B. Procedural History.

The sole issue before the district court was whether to grant the defendants' motion to suppress the extensive CSLI obtained by the government.[72] The defendants argued that "the length of time and extent" of cell phone monitoring conducted by the government was unconstitutional because it violated the Fourth Amendment's protection against unreasonable searches and seizures.[73] The First Order authorized the release of fourteen days and 1628 individual CSLI data points.[74] The Second Order authorized the release of 221 days and 20,235 individual CSLI data points.[75] The defendants

63. 18 U.S.C. § 2703(d) (2012).
64. *Graham*, 846 F. Supp. 2d at 386.
65. *Id.*
66. *Id.* at 386–87.
67. *Id.* at 387.
68. *Id.* This application included the same dates from the First Order. *Id.*
69. *Id.*
70. *Id.*
71. *Id.* at 385.
72. *Id.*
73. *Id.* at 387.
74. *Id.*
75. *Id.*

argued that such an extensive collection of data permits the government "to paint an intimate picture of the defendants' whereabouts."[76] Moreover, this type of technology effectively allows the government to "retroactively track or surveil a suspect through his cellular telephone, a device he likely carries with him at all hours of the day."[77]

The district court ultimately concluded that the defendants did not have a "legitimate expectation of privacy" in the CSLI acquired by the government and thus denied the defendants' motion to suppress.[78] The court principally relied on the "third-party doctrine" posited in *Smith v. Maryland*.[79] In *Smith*, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[80] Because the defendants voluntarily conveyed CSLI to Sprint/Nextel, the defendants similarly had no legitimate expectation of privacy in such data.[81]

In reaching this conclusion, the district court analogized the transmission of CSLI to Supreme Court precedent regarding the transmission of financial records and telephone numbers.[82] In *United States v. Miller*,[83] the Supreme Court held that individuals do not have a legitimate expectation of privacy in financial records held by a bank.[84] When an individual provides financial information to a bank, he voluntarily conveys such information to the bank for it to retain as part of its business records.[85] By doing so, the individual voluntarily assumes the risk that such information would be conveyed to the government.[86] In *Smith*, the Supreme Court similarly concluded that the installation and use of a pen register did not violate the Fourth Amendment.[87] When an individual dials a phone to place a phone call, he voluntarily conveys the numerical information to the telephone company.[88] Therefore, he assumes the

---

76. *Id.*
77. *Id.*
78. *Id.* at 389.
79. *See id.* at 397–99.
80. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
81. *See Graham*, 846 F. Supp. 2d at 399–401.
82. *Id.* at 398. A pen register, also known as a dialed number recorder, is a device that records all numbers dialed into a particular telephone. S. REP. No. 1097, 90th Cong., 2d Sess. 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153–54.
83. 425 U.S. 435 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422, *as recognized in* Popoli v. Ft. Myers Lodge #1899 Loyal Order of Moose, Inc., No. 2:15-cv-311-FtM-29CM, 2015 WL 9031929, at *4 (M.D. Fla. Dec. 16, 2015).
84. *Id.* at 442–43.
85. *Id.*
86. *Id.* at 443.
87. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).
88. *Id.* at 742.

risk that the telephone company would reveal such information to the government.[89]

Similarly, the district court noted that cell phone users voluntarily convey CSLI when they place a phone call.[90] Cell phone companies retain information "that identifies the cellular towers through which a person's calls are routed" as part of their ordinary course of business.[91] Cell phone users "must" realize they convey such data in order for the cellular service provider to complete the users' phone calls.[92] In fact, Sprint/Nextel's privacy policy even informs its customers that it collects and stores location data.[93] Furthermore, the records do not pinpoint a specific address, but rather only identify the closest cell tower.[94] Therefore, the court concluded that the defendants voluntarily conveyed the CSLI and denied the defendants' motion to suppress.[95]

III. THE FOURTH CIRCUIT'S DECISION IN *UNITED STATES V. GRAHAM*

After the defendants' motion to suppress was denied, the case proceeded to trial.[96] The government introduced the CSLI at trial to establish the defendants' locations at various times surrounding the charged robberies.[97] Aaron Graham was ultimately convicted of being a felon in possession of a firearm, Hobbs Act robbery, conspiracy to commit Hobbs Act robbery, and brandishing a firearm in connection with six robberies that occurred between January 17, 2011, and February 5, 2011.[98] Eric Jordan was convicted of conspiracy, Hobbs Act robbery, and handling a firearm in connection with three of these robberies.[99] Both defendants subsequently appealed their convictions, once again challenging the admissibility of CSLI obtained by the government.[100] Recognizing several fallacies in the district court's analysis, the Fourth Circuit concluded that the "warrantless procurement" of CSLI constituted an unreasonable search in violation of the Fourth Amendment.[101]

While the Fourth Circuit addressed several bases for appeal in *Graham*, this Part specifically focuses on the Fourth Circuit's

---

89. *Id.* at 744.
90. United States v. Graham, 846 F. Supp. 2d 384, 399 (D. Md. 2012).
91. *Id.* at 400.
92. *Id.* at 401.
93. *Id.*
94. *Id.* at 404.
95. *See id.* at 399, 406.
96. United States v. Graham, 796 F.3d 332, 341 (4th Cir. 2015).
97. *Id.* at 342–43.
98. *Id.* at 339.
99. *Id.*
100. *Id.* at 338.
101. *Id.* Nevertheless, the Fourth Circuit upheld the conviction of the defendants because the government acted in good faith reliance on court orders issued under the SCA. *Id.*

Fourth Amendment analysis regarding the procurement of CSLI.[102] In concluding that the government conducts a search under the Fourth Amendment when it procures a cell phone user's historical CSLI, the Fourth Circuit focused on two main points: (1) the extent of information collected by CSLI; and (2) the cell phone user's reasonable expectation of privacy related to the third-party doctrine.[103] This part will now discuss each of these points in turn.

A. The Extent of Information Collected by CSLI

The first major issue that the Fourth Circuit addressed regarding the warrantless procurement of CSLI was the extent of personal information that such historical information provides.[104] "The Supreme Court has recognized an individual's privacy interests in comprehensive accounts of her movements . . . particularly when such information is available only through technological means not in use by the general public."[105] The Supreme Court first addressed long-term electronic location surveillance in *United States v. Jones*.[106]

In *Jones*, the Supreme Court addressed the constitutionality of the government's installation of a GPS device in a suspect's vehicle to track its movements over a twenty-eight-day period.[107] In concluding that such installation constituted a search under the Fourth Amendment, the majority confined its analysis to the traditional trespass-based theory of Fourth Amendment protection.[108] Nevertheless, in total, five Justices addressed the privacy interests implicated through long-term GPS monitoring.[109] In both the majority and concurring opinions, the five Justices agreed that long-term aggregation of an individual's movements through technological advancements "impinges on expectations of privacy."[110]

Recognizing this precedent, the Fourth Circuit concluded that the collection of CSLI over an extended period of time affects privacy interests to an even greater extent than GPS monitoring.[111] Like GPS monitoring, CSLI reveals "both a comprehensive view and

---

102. *Id.* at 342.
103. *See id.* at 344–45.
104. *See id.* at 345–51.
105. *Id.* at 345.
106. 132 S. Ct. 945 (2012).
107. *Id.* at 948.
108. *See id.* at 949–54.
109. *See id.* at 954–57 (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring).
110. *Id.* at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring)).
111. United States v. Graham, 796 F.3d 332, 348 (4th Cir.), *reh'g granted*, 642 Fed. App'x 75 (4th Cir. 2015) (mem.).

specific details of the individual's daily life."[112] It not only permits one to infer where an individual lives,[113] but also where he goes to church or the gym, how he receives medical treatment, and even what his sexual habits are.[114] Even worse, CSLI can provide an even more comprehensive picture of one's life. A cell phone is often carried by the user and rarely leaves his presence.[115] Cell phones are thus carried throughout public and private places, where a vehicle has limited or no access.[116]

In fact, in this case, the available CSLI provided 29,659 data points for Aaron Graham and 28,410 data points for Eric Jordan over a 221-day period.[117] This amounts to an average of over 100 data points per defendant per day.[118] Some of these data points could cover areas as small as forty feet.[119] The long-term collection of such precise information led the Fourth Circuit to conclude that the government conducted a search under the Fourth Amendment, and thus, the government must demonstrate probable cause and acquire a search warrant to obtain such data.[120]

B. Reasonable Expectation of Privacy Related to the Third-Party Doctrine

The second major issue the Fourth Circuit addressed was whether the defendants had a reasonable expectation of privacy in their CSLI because it was kept by Sprint/Nextel in its ordinary course of business.[121] In other words, the Fourth Circuit had to address whether the third-party doctrine applied to a service provider's collection of CSLI. As noted earlier, the district court concluded that the third-party doctrine did apply.[122] The Fourth Circuit, however, refused to apply the doctrine because the defendants did not "voluntarily convey" their CSLI.[123]

As previously noted, Supreme Court precedent has established that an individual does not have a reasonable expectation of privacy when he provides financial information to a bank or dials numbers

---

112. *Id.*
113. *Id.* at 346.
114. *Id.* at 348 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010); State v. Earls, 70 A.3d 630, 642 (N.J. 2013)).
115. *Id.*
116. *Id.*
117. *Id.* at 350.
118. *Id.*
119. *Id.* at 350–51.
120. *Id.* at 344–45.
121. *See id.* at 351–53.
122. *Id.* at 400.
123. United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012), *aff'd*, 796 F.3d 332, 354 (4th Cir. 2015), *reh'g granted*, 642 Fed. App'x 75 (4th Cir. 2015) (mem.).

to place a phone call.[124] The Fourth Circuit distinguished the present case from this precedent by focusing on the "voluntary conveyance" of such information.[125] In the aforementioned examples, the individual must take some form of voluntary, affirmative action.[126] At a bank, an individual exchanges his financial information for services provided by the bank. In order to place a call, an individual voluntarily presses numbers on a phone.

Cell phone providers, however, automatically collect CSLI, regardless of whether the user actively participated in its transmission.[127] Moreover, CSLI is neither tangible nor visible to the user.[128] Location identifying information is not only collected when a call or message is placed, but also when calls and messages are received and unanswered.[129] Simply because CSLI "winds up in the third party's records" is insufficient to impute that a cell phone user lacked a reasonable expectation of privacy, particularly when this information is automatically generated by the service provider without the user's involvement.[130]

Furthermore, the Fourth Circuit found the evolution and importance of cell phone technology in today's society at odds with the outdated third-party doctrine.[131] "Cell phone use . . . has become essential to full cultural and economic participation."[132] It cannot be assumed that all cell phone users consent to "warrantless government access" simply by choosing to carry a cell phone.[133] Should that be the case, the government could effectively convert everyone's cell phones into tracking devices, even without probable cause.[134] As technology evolves, Fourth Amendment jurisprudence must remain consistent and, if necessary, adapt to society's reasonable expectations of privacy.[135] For these reasons, the Fourth Circuit refused to apply the third-party doctrine and held that the

---

124. Smith v. Maryland, 442 U.S. 735, 744–45 (1978).

125. *Graham*, 796 F.3d at 354.

126. *Smith*, 442 U.S. at 744; United States v. Miller, 425 U.S. 435, 442 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422, *as recognized in* Popoli v. Ft. Myers Lodge #1899 Loyal Order of Moose, Inc., No. 2:15-cv-311-FtM-29CM, 2015 WL 9031929, at *4 (M.D. Fla. Dec. 16, 2015).

127. *Graham*, 796 F.3d at 354.

128. *Id.* at 355.

129. *Id.*

130. *Id.* at 354–55.

131. *Id.* at 360.

132. *Id.* at 355–56.

133. *Id.* at 356 (quoting *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011)).

134. *Id.* at 357.

135. *Id.* at 359.

defendants had "a reasonable expectation of privacy in their long-term CSLI."[136]

IV. AFTER *GRAHAM*: THE RESULTING CIRCUIT SPLIT

The Fourth Circuit's decision in *Graham* created a circuit split regarding whether the warrantless procurement of CSLI violated the Fourth Amendment.[137] The Third, Fifth, and Eleventh Circuits all reached the opposite conclusion that a warrant is not required to obtain CSLI.[138] Many district court and state supreme court decisions have similarly fallen on both sides of this issue.[139] This Part addresses this circuit split and briefly discusses other district court and state supreme court decisions.

A. Fifth Circuit

In *In re Application of the United States for Historical Cell Site Data*,[140] the Fifth Circuit concluded that the production of historical CSLI in accordance with the SCA does not per se violate the Fourth Amendment.[141] In reaching this decision, the Fifth Circuit specifically focused on the third-party doctrine.[142] First, the Fifth Circuit concluded that CSLI is a business record.[143] CSLI is collected by service providers for a variety of business purposes, such as optimizing services or routing phone calls.[144] In contrast to the Fourth Circuit, the Fifth Circuit noted that cell phone users take voluntary, affirmative action by paying service providers to provide exactly these services.[145] The service providers then collect location information on their own volition, rather than at the instruction of

---

136. *Id.* at 360.

137. *Compare id.* at 360–61 (holding that collection of CSLI was a search that violated the Fourth Amendment), *with* United States v. Davis, 785 F.3d 498, 513 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015) (holding that collection of CSLI was not a search and did not violate the Fourth Amendment).

138. *See Davis*, 785 F.3d at 518; *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 an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

139. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (holding that the SCA and Pen/Trap Statute do not permit the government to obtain CSLI without a warrant); Tracey v. State, 152 So. 3d 504, 525–26 (Fla. 2014) (holding that collection of CSLI without a warrant violated the Fourth Amendment); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (holding that collection of CSLI without a warrant violated the New Jersey Constitution).

140. 724 F.3d 600.

141. *Id.* at 602.

142. *See id.* at 610.

143. *Id.* at 611.

144. *Id.* at 611–12.

145. *Id.* at 612.

the government.[146] The government simply comes in after the fact and requests that the service provider turn over these previously created records.[147]

Second, the Fifth Circuit concluded that cell phone users voluntarily convey their CSLI to service providers.[148] Cell phone use is completely voluntary.[149] Neither the government, nor anyone else for that matter, requires an individual to utilize a cell phone.[150] Cell phone users generally understand that a cell phone must connect to a nearby cell tower in order to connect the phone.[151] Moreover, many service providers indicate in their privacy policies that they collect location information and will disclose it to the government upon a court order.[152] The Fifth Circuit thus concluded that cell phone users cannot have a reasonable expectation of privacy in their CSLI. As such, the SCA does not per se violate the Fourth Amendment.[153]

B. Eleventh Circuit

The Eleventh Circuit similarly held in *United States v. Davis*[154] that government obtainment of CSLI under the SCA does not violate the Fourth Amendment.[155] Like the Fifth Circuit, the Eleventh Circuit applied the third-party doctrine.[156] The Eleventh Circuit noted that the defendant had no ownership or possession interest in MetroPCS's business records; MetroPCS created, controlled, and stored these documents on its own premises.[157] The Eleventh Circuit also agreed with the Fifth Circuit that users cannot have a reasonable expectation of privacy regarding CSLI.[158] Cell phone users know that in order for their cell phone to work it must be connected to a service tower within range.[159] Therefore, the Eleventh Circuit concluded that cell phone users cannot even have an objective expectation of privacy, and the production of CSLI under the SCA does not violate the Fourth Amendment.[160]

However, this case importantly included some rather significant facts that distinguished it from *Graham* and other circuit court

146. *Id.*
147. *Id.*
148. *Id.* at 613.
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.* at 615.
154. 785 F.3d 498 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015).
155. *Id.* at 511.
156. *See id.*
157. *Id.*
158. *Id.*
159. *Id.*
160. *Id.* at 511–13.

decisions. First, the defendant's cell phone service provider, MetroPCS, only provided information related to: incoming and outgoing phone calls; their respective dates, times, and durations; and the location of cell towers to which the cell phone was connected during the calls.[161] Second, MetroPCS did not provide any information relating to incoming or outgoing text messages, or location information collected when the phone was on but not in use.[162] Had the CSLI data set been as extensive as the one the Fourth Circuit addressed in *Graham*, the Eleventh Circuit may have very well reached a different conclusion.

C. Third Circuit

The Third Circuit addressed the warrantless procurement of CSLI in *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government.*[163] In this case, a magistrate judge denied the government's application for an order to compel a service provider to produce CSLI, despite the fact that the government offered the requisite "specific and articulable facts" required under the SCA.[164] The magistrate judge held the government to the higher "probable cause" standard because it concluded that a cell phone operates like a tracking device.[165] The government appealed this decision, arguing that once the government meets the SCA requirements, a magistrate judge must grant an order to compel.[166]

Compared to the Fifth and Eleventh Circuits, the Third Circuit seems to have struck more of a middle ground regarding the government procurement of CSLI. The Third Circuit rejected the magistrate judge's conclusion that cell phones operate as tracking devices.[167] While the Third Circuit agreed that electronic communications such as tracking devices are excluded from the SCA, the court held that CSLI and cell phones actually involve wire communication.[168] As such, CSLI falls under the SCA, and the "specific and articulable facts" standard applies.[169] However, the Third Circuit was not prepared to completely hold that the probable cause standard could never apply to CSLI.[170] Instances may arise where the types of location information requested by the government implicate Fourth Amendment concerns.[171] The

161. *Id.* at 502.
162. *Id.* at 503.
163. 620 F.3d 304, 305 (3d Cir. 2010).
164. *Id.* at 305–06, 308.
165. *Id.* at 308–09.
166. *Id.* at 315.
167. *Id.* at 312–13.
168. *Id.* at 309–10.
169. *Id.* at 313.
170. *Id.* at 319.
171. *See id.* at 317.

magistrate judge must have the discretion to make these decisions.[172] Nevertheless, the Third Circuit cautioned that any departure must be used sparingly and based on full factual findings and explanations.[173]

D. Other District Court and State Supreme Court Decisions

Several other district courts and state supreme courts have similarly addressed whether the warrantless procurement of CSLI violates the Fourth Amendment and have reached contrary conclusions. For instance, the Eastern District of New York and the Massachusetts Supreme Court have agreed with the Fourth Circuit that the warrantless procurement of CSLI violates the Fourth Amendment.[174] In *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*,[175] the government requested 113 days of CSLI.[176] Like the Fourth Circuit, the Eastern District of New York concluded that cell phone users have a reasonable expectation of privacy regarding such long-term location records.[177] Therefore, consistent with the Fourth Amendment, the government must obtain a warrant to procure such extensive CSLI.[178] The Massachusetts Supreme Court reached a similar conclusion in *Commonwealth v. Augustine*[179] by specifically focusing on the unsuitable application of the third-party doctrine in the current digital age.[180]

On the other hand, the District of Kansas and the North Carolina Court of Appeals have agreed with the Third, Fifth, and Eleventh Circuits that the warrantless procurement of CSLI does not violate the Fourth Amendment.[181] In *United States v. Banks*,[182] the District of Kansas distinguished a "preference" that CSLI

---

172. *See id.* at 316–17.

173. *Id.* at 319. In contrast, the Fifth Circuit afforded no discretion to magistrate judges to hold the government to the higher probable cause standard. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 607 (5th Cir. 2013). The Fifth Circuit emphasized the language of the SCA, that based upon a showing of specific and articulable facts, the magistrate judge *shall* grant an order. *Id.*

174. *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011); Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014) (stating that Fourth Amendment jurisprudence is unclear in regard to CSLI and deciding the case on state constitutional grounds).

175. 809 F. Supp. 2d 113.

176. *Id.* at 118.

177. *Id.* 119–20.

178. *Id.* at 127.

179. 4 N.E.3d 846 (Mass. 2014).

180. *See id.* at 857–66.

181. *See* United States v. Banks, 52 F. Supp. 3d 1201, 1206 (D. Kan. 2014); State v. Perry, 776 S.E.2d 528, 540 (N.C. Ct. App. 2015).

182. 52 F. Supp. 3d 1201.

remain private from a reasonable expectation that CSLI is in fact private.[183] Cell phone service providers openly collect and record CSLI.[184] Consequently, the defendants could not have a reasonable expectation that their CSLI would remain private.[185] Even the North Carolina Court of Appeals was unconvinced by the precedent established by the Fourth Circuit in *Graham*.[186] In *State v. Perry*,[187] the court distinguished *Graham* by noting that the government sought information for only portions of two days rather than the 221 days requested in *Graham*.[188] Therefore, like the Third, Fifth, and Eleventh Circuits, the Court applied the third-party doctrine and held that the defendant did not have a reasonable expectation of privacy in his CSLI.[189]

V. ANALYSIS

In this Part, I argue that the warrantless procurement of CSLI violates the Fourth Amendment to the U.S. Constitution. As noted earlier, in *Jones*, the majority opinion, authored by Justice Scalia, concluded that the transmission of electronic signals remains subject to the *Katz* analysis.[190] The first part of my argument thus proceeds by concluding that individuals have a subjective expectation that their CSLI will remain private and that this expectation is reasonable. Next, because many courts—particularly, the Third and Fifth Circuits—have applied the third-party doctrine to conclude that the warrantless procurement of CSLI does not implicate Fourth Amendment protections, I argue that the application of the third-party doctrine to the collection of such data is inappropriate.

A. Individuals Have a Subjective Expectation that CSLI Will Remain Private and that Expectation Is Reasonable

First, individuals have a subjective expectation that CSLI collected by service providers will remain private. A recent survey conducted by the Pew Research Center found that fifty percent of adults believe that details of their physical location gathered over a period of time through GPS on a cell phone is "very sensitive" information, and another thirty-two percent considered this data "somewhat sensitive."[191] When consumers were asked if they lost

183. *Id.* at 1206.
184. *Id.*
185. *Id.*
186. *Perry*, 776 S.E.2d at 540.
187. 776 S.E.2d 528.
188. *Id.* at 540.
189. *See id.* at 538–40.
190. *See supra* notes 37–41 and accompanying text.
191. MARY MADDEN ET AL., PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 34 (2014),

control over how personal information is collected and used by companies, ninety-one percent of adults "agreed" or "strongly agreed."[192] In addition, eighty percent of adults "agreed" or "strongly agreed" that Americans should be concerned about the government's monitoring of phone calls and internet communications.[193]

If that is how Americans feel about cell phone GPS data and the government collection of data generally, imagine how many Americans would react if they discovered the government could procure 221 days of CSLI to track their every movement. Then, imagine how those same people would react once they discovered this data can be obtained without a warrant. The reality is, CSLI is the functional equivalent of GPS tracking. It allows the government to paint an intimate portrait of your life. The government can determine where you live, where you go to church, what your political affiliations are, and more. The government can even determine important and personal life achievements. For instance, in *Graham*, the American Civil Liberties Union ("ACLU") analyzed the same CSLI provided to the government.[194] Based on this data, the ACLU was able to conclude that Aaron Graham's wife was pregnant.[195]

In 2014, AT&T received 64,703 requests for CSLI.[196] Six months into 2015, Verizon received more than 21,000 requests.[197] This amounts to over 100 requests per day per carrier.[198] Ironically, the one person these carriers will not provide this information to is the user herself. That is right, the only way to obtain one's own personal CSLI is through a court order.[199] And then, the information is given to law enforcement, not the user.[200] Courts need to start addressing this "process" for what it is: a joke. Even the government has been rather candid as to the purpose of this data. The government considers this data a "building block" to its

---

http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

192. *Id.* at 3.

193. *Id.*

194. Bennet Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013, 4:16 PM), https://www.aclu.org/blog/fighting-striking-case-warrantless-cell-phone-tracking.

195. *Id.*

196. Meyer, *supra* note 4.

197. *Id.*

198. *Id.*

199. *See* Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data—Just Not with You*, PROPUBLICA (June 26, 2012, 2:44 PM), http://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

200. *See id.*

investigation, like chatting with bystanders.[201] Personally, I am not aware of a bystander who, after witnessing a crime, proceeded to follow the "perpetrator" twenty-four hours a day for 221 days and document all 29,659 locations he traversed. It is hard to believe, under any circumstance, that an individual would not have a subjective belief that this amount of data would remain private.

Second, this subjective belief is deemed reasonable by society. While the previously discussed statistical evidence shows that this subjective belief is reasonable, the importance of cell phones in today's society further supports this notion. "Cell phone use is not only ubiquitous in our society . . . it has become essential to full cultural and economic participation."[202] Before the digital age, people did not carry "a cache of sensitive personal information with them as they went about their day."[203] Today, cell phones are not simply devices used to place or receive calls, they are "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, [and] newspapers."[204] Ninety percent of American adults today own a cell phone, sixty-four percent of whom own a smartphone.[205] Cell phones are often carried throughout the day in one's pocket or purse. In fact, nearly three-quarters of individuals claim to be within five feet of their phones at all times.[206] We as a society have become so attached to our phones, we even sleep next to them and take them in the shower.[207] Society clearly has an objectively reasonable basis to believe that CSLI will remain private. To conclude otherwise is, quite simply, ridiculous.

B. The Third-Party Doctrine Is Inapplicable to the Collection of CSLI

Many courts have circumvented the *Katz* analysis through the third-party doctrine.[208] The third-party doctrine posits that an individual has no legitimate expectation of privacy in information he voluntarily turns over to third parties.[209] In turn, because the individual does not have a legitimate expectation of privacy, the

---

201. *See* Supplemental Brief of Appellee United States of America at 4–5, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (No. 12-4659 (L)), 2014 WL 3772867.

202. United States v. Graham, 796 F.3d 332, 355–56 (4th Cir.), *reh'g granted*, 624 F. App'x 75 (4th Cir. 2015) (mem.).

203. Riley v. California, 134 S. Ct. 2473, 2490 (2014).

204. *Id.* at 2489.

205. *Mobile Technology Fact Sheet*, PEW RES. CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Apr. 14, 2016) [http://web.archive.org/web/20160223051253/http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/].

206. *Riley*, 134 S. Ct at 2490.

207. *Id.*; PEW RES. CTR., *supra* note 205.

208. *See supra* Part IV.

209. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

doctrine does not implicate Fourth Amendment concerns. This doctrine is problematic for two main reasons. First, this doctrine is incredibly outdated and based on the technology available during the 1970s. Second, an individual does not "voluntarily convey" CSLI to service providers; cell phone users are forced to convey this information.

The third-party doctrine arose out of *Miller*, where the Supreme Court held that an individual does not have a reasonable expectation of privacy in financial records created by the bank.[210] These records were owned by the bank and pertained to transactions to which the bank was a party.[211] The Supreme Court reaffirmed this principle in *Smith*, by holding that an individual did not have a reasonable expectation of privacy to numbers recorded in a pen register.[212] Unfortunately, courts have continued to blindly apply this doctrine ever since.

The third-party doctrine is premised on the fact that "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[213] However, *Miller* was decided in 1976.[214] The first Apple computer just hit the market that year.[215] The cell phone would not make its commercial appearance for another seven years.[216] And when *Smith* was decided, only the numbers dialed into the phone were recorded by the pen register.[217] Technology today allows companies to collect a whole host of data, even when the user is not using his cell phone.[218] The Supreme Court was not equipped to fathom the concerns the digital age would present, and consequently, the third-party doctrine is ill-suited for the present day.

Additionally, simply because a service provider *can* determine one's location based on a phone call does not mean the individual

---

210. United States v. Miller, 425 U.S. 435, 440 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422, *as recognized in* Popoli v. Ft. Myers Lodge #1899 Loyal Order of Moose, Inc., No. 2:15-cv-311-FtM-29CM, 2015 WL 9031929, at *4 (M.D. Fla. Dec. 16, 2015).

211. *Id.* at 440–41.

212. *Smith*, 442 U.S. at 745–46.

213. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citing *Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 443).

214. *Miller*, 425 U.S. at 435.

215. Dan Knight, *Personal Computer History: The First 25 Years*, LOW END MAC (Apr. 26, 2014), http://lowendmac.com/2014/personal-computer-history-the-first-25-years/.

216. *See* Zachary M. Seward, *The First Mobile Phone Call Was Made 40 Years Ago Today*, ATLANTIC (Apr. 3, 2013), http://www.theatlantic.com/technology/archive/2013/04/the-first-mobile-phone-call-was-made-40-years-ago-today/274611/.

217. *See Smith*, 442 U.S. at 741.

218. Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES (Mar. 26, 2011), http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=0.

waives the privacy of that information. At some point, a line must be drawn between what an individual voluntarily conveys and what he is forced to convey. This leads me to my second point: cell phone users do not voluntarily convey CSLI to cell phone service providers.

According to the Merriam-Webster dictionary, the first three definitions of voluntary are: "(1) proceeding from the will or from one's own choice or consent; (2) unconstrained by interference . . . ; [and] (3) done by design or intention."[219] Can you remember ever requesting that your service provider record your location every time you make call, send a text message, download an application, or when your phone "registers" with a service tower? Furthermore, when did service providers begin recording CSLI, and why is it necessary? Thus far, my research has not uncovered when cell phone companies specifically began compiling a physical record of every user's CSLI. However, one purpose to record such data is so that service providers may optimize their networks.[220] The question still remains, why must the service provider record one's personal CSLI? It seems equally plausible that a service provider can achieve the same results anonymously.

Nevertheless, the reality is that service providers automatically record CSLI.[221] There is nothing you or I can do to prevent this from happening. It is the byproduct of owning a cell phone. Thus, the only option that remains is to refrain from owning a cell phone. However, market realities prohibit this from being a realistic option. Many companies require employees to carry a business phone.[222] Even if it is not a requirement, employers certainly prefer, or at least appreciate, employees who are easily accessible through a cell phone. Accordingly, cell phone use truly is "essential to full cultural and economic participation."[223]

The argument often put forward is that cell phone users "consent" to the recording of CSLI once the user signs a service contract.[224] These service contracts include privacy policies that disclose to the user that such data are recorded.[225] First, this does not inform users that CSLI will be provided to the government or other individuals upon request. Second, this returns cell phone users to their only alternative option, to refrain from owning a cell phone. There is nothing voluntary about this arrangement. Cell

---

219. *Voluntary*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/voluntary (last visited Apr. 14, 2016).

220. United States v. Banks, 52 F. Supp. 3d 1201, 1206 (D. Kan. 2014) (quoting *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013)).

221. Meyer, *supra* note 4.

222. Chamberlain, *supra* note 12, at 1786.

223. United States v. Graham, 796 F.3d 332, 355–56 (4th Cir.), *reh'g granted*, 624 F. App'x 75 (4th Cir. 2015) (mem.).

224. *See id.* at 345.

225. *See id.*

phone users do not have a viable choice in the matter. A majority of Americans believe it would be difficult to adopt tools and strategies to protect their privacy on their cell phones.[226] Many individuals are not even aware such tools exist or do not think they apply, despite the fact they own a cell phone.[227] Cell phone users are thus constrained, forced to permit the recording of CSLI or otherwise sacrifice full cultural and economic participation. The third-party doctrine ignores this reality. Therefore, it is inapplicable to the collection of CSLI.

CONCLUSION

The Fourth Amendment was enacted to strip the government of the "unfettered authority" to search through an individual's personal belongings in the hope of finding something incriminating.[228] It was designed to make law enforcement's job more difficult. Therefore, as the Fourth Circuit so eloquently stated, "If the Twenty-First Century Fourth Amendment is to be a shrunken one . . . we should leave that solemn task to our superiors in the majestic building on First Street . . . ."[229]

Unfortunately, it seems most courts are taking the opposite approach and shrinking the protections of the Fourth Amendment. The Fourth Circuit vacated the majority decision in *Graham* pending a rehearing en banc.[230] The Supreme Court recently denied certiorari to *Davis,* and thus gave up its opportunity to address the constitutionality of the warrantless procurement of CSLI.[231] Many courts have requested that Congress address this issue, yet Congress continues to sit idly by, twiddling its thumbs, while increasingly more Americans are subject to the technological equivalent of a full rectal exam.[232] Quite frankly, courts must realize that Congress is simply not interested in helping. The Fourth Circuit currently has the opportunity to reaffirm the protections of the Fourth Amendment and hold that the warrantless

---

226. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

227. *Id.*

228. Rand Paul & Chris Coons, *The Founding Fathers Would Have Protected Your Smartphone*, POLITICO MAG. (May 27, 2014), http://www.politico.com/magazine/story/2014/05/a-tech-challenge-for-fourth-amendment-application-107129.

229. *Graham*, 796 F.3d at 361.

230. United States v. Graham, 624 F. App'x 75, 75 (4th Cir. 2015) (mem.).

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

232. *See, e.g.*, *Graham*, 796 F.3d at 361; United States v. Davis, 785 F.3d 498, 512 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015); *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 an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

procurement of CSLI is unconstitutional.[233] The Fourth Circuit should heed the Supreme Court's concerns in *Jones* and *Riley* and do just that.

Steven M. Franklin[*]

233. *Graham*, 624 F. App'x at 75.

* Wake Forest University School of Law, J.D. Candidate, 2016; North Carolina State University, B.A. Political Science, 2013. The author would like to thank his parents, Mike and Simone Franklin, his sister, Kelly Franklin, and Shannon Crawford for their unwavering love and support, even despite all odds. The author would also like to thank Professor Ronald Wright for helpful direction and insight, and all *Wake Forest Law Review* board and staff members for their outstanding work and dedication.

***