Fordham Law Review

Volume 85 | Issue 5 Article 19

2017

The Fourth Amendment, CSLI Tracking, and the Mosaic Theory

Christian Bennardo
Fordham University School of Law

NOTES

THE FOURTH AMENDMENT, CSLI TRACKING, AND THE MOSAIC THEORY

*Christian Bennardo**

Law enforcement officials and privacy advocates have long clashed over the police's ability to access and use information related to cell phones during criminal investigations. From wiretapping to physical searches of phones, the competing investigatory and privacy interests continue to battle for priority on a number of different fronts. This Note addresses the disagreement between academic scholarship and federal circuit courts over the proper resolution to one particular issue: cell site location information (CSLI).

CSLI refers to the records kept by a cellular service provider indicating the approximate location of a customer's phone over time. Police often procure CSLI from providers to track a suspect's movements in relation to criminal activity. However, when they do so without a warrant, courts are forced to determine whether the police violated the suspect's Fourth Amendment right against unreasonable searches.

To date, all of the circuit courts to address this issue have held that warrantless CSLI monitoring is permitted under the Fourth Amendment. Many scholars, however, argue to the contrary, criticizing these decisions and creating a rift between the academic and judicial treatment of CSLI.

This Note explores the CSLI debate by analyzing the circuit courts' decisions, scholars' disagreement with those decisions, and the alternative approaches offered to protect and evaluate CSLI records. This Note concludes that warrantless CSLI monitoring should be analyzed under the "mosaic theory" of the Fourth Amendment. In support, it argues that this theory best addresses the concerns with CSLI tracking and proposes a standard that courts may use to apply it.

* J.D. Candidate, 2018, Fordham University School of Law; B.A., 2015, Villanova University. Thank you to Professor Martin S. Flaherty for his invaluable advice and encouragement throughout this process. I would also like to thank my family for their unconditional love and support.

INTRODUCTION

By the time you sat down to read this Note today, you likely used your cell phone to make a number of calls, to send many more text messages and emails, and to refresh your Facebook, Instagram, and Twitter accounts. If you paid your latest bill, your cellular service provider was happy to make all of these actions possible. However, while you were busy staying connected with family and friends, your service provider was also hard at work: recording your location—one phone call, text message, and social media post at a time.

In fact, service providers approximate and record the location of the cell phones that they service even when their owners are not actively using them.[1] Any time a cell phone is turned on, it automatically identifies and registers with the nearest cell tower—also called a cell site—every seven seconds in

1. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 736 (2011).

order to communicate.[2] At each registration, the provider obtains and records a "plethora of information" about the phone, including its approximate location relative to the cell site with which it registered.[3] This data is known as cell site location information (CSLI).

Because cell phones constantly connect with the nearest tower, providers possess an almost complete record of a phone's location over a given time period.[4] As a result, law enforcement officials often obtain and use CSLI during criminal investigations to locate a suspect near the scene of a recent crime or to track his movements in relation to a series of crimes.[5]

Generally speaking, law enforcement's ability to access and use cell-phone-related information has given rise to a number of questions about the amount of privacy individuals have with their phones: How much of what users say is private? What about how they said it or to whom they said it? Is it reasonable to expect privacy in today's advanced digital era? And lastly, do users have any protection from those who wish to access this information? Questions like these are not novel inquiries. However, the individuals and institutions considering these issues do not always agree on how to resolve them. CSLI falls into this category.

In particular, many courts have had to address whether the government may obtain and use CSLI from an individual's service provider without a search warrant. To date, all of the federal circuit courts to confront this issue have held that warrantless CSLI monitoring is not a Fourth Amendment violation.[6] As these decisions have been handed down, however, both scholars and students have considered the issue and analyzed specific cases appearing before the courts.[7] Significantly, these commentators are largely critical of the circuit courts' holdings and rationales[8] and advocate for protection of CSLI under the Fourth Amendment.[9] These criticisms create a divisive split between judicial and academic treatment of warrantless CSLI

2. *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 5 (2013).

3. *Id.*

4. *See* Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 805–06 (2013).

5. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016) (noting that the government obtained a CSLI for seven months); United States v. Graham, 796 F.3d 332, 342 (4th Cir. 2015) (noting that the government obtained CSLI for 221 days from the defendants' service providers), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); United States v. Davis, 785 F.3d 498, 501 (11th Cir. 2015) (noting that the government obtained CSLI for sixty-seven days); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) [hereinafter *Historical Cell Site Data Case*] (noting that government requested CSLI for a two-month time period).

6. *See Graham*, 824 F.3d at 424; *Carpenter*, 819 F.3d at 890; *Davis*, 785 F.3d at 500; *Historical Cell Site Data Case*, 724 F.3d at 615; *In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 313 (3d Cir. 2010) (holding that while warrantless procurement of CSLI is not a per se violation of the Fourth Amendment, a magistrate has the option to require the government to obtain a warrant in some circumstances).

7. *See infra* Part II.B–C.

8. *See infra* Part II.B.

9. *See infra* Part II.C.

tracking, a split that circuits that have yet to address the issue will have to consider when CSLI-related cases appear on their dockets.

This Note addresses whether law enforcement officials should be required to obtain a warrant before procuring CSLI records to monitor an individual's movements. Part I discusses the U.S. Supreme Court's Fourth Amendment jurisprudence and then explains the mechanics of CSLI and how law enforcement currently obtains this information under the Stored Communications Act (SCA).[10] Then, Part II articulates the disagreement between the federal appellate judiciary and academia over the warrantless procurement of CSLI, and it outlines the alternative approaches that commentators have proposed to protect and analyze CSLI.

Part III seeks to reconcile the competing arguments in the debate over the warrantless use of CSLI records. It argues that courts should apply the "mosaic theory" of the Fourth Amendment to determine the constitutionality of CSLI monitoring. In doing so, this part joins other scholars who advocate for the theory, explains why it is best suited to address the underlying concerns with CSLI disclosure, and adds to the discussion by proposing a standard under which courts may apply the mosaic theory to CSLI. Lastly, this part recognizes that the standard it offers does not solve all of the problems that arise when implementing this theory. Nonetheless, the standard can serve as an initial step toward creating a more complete, viable framework that permits the application of the mosaic theory to CSLI tracking.

I. THE FOURTH AMENDMENT, CSLI, AND THE SCA

This part explains the U.S. Supreme Court's Fourth Amendment jurisprudence, the mechanics and details of CSLI, and how law enforcement obtains this information under the SCA.

A. Katz *and Fourth Amendment Searches*

The Fourth Amendment of the U.S. Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches."[11] Traditionally, the Fourth Amendment protected only against governmental searches that "physically intruded" upon an individual's body or property.[12] However, in *Katz v. United States*,[13] the Supreme Court expanded the Fourth Amendment's protections and held that a search can occur even absent physical trespass.[14]

10. 18 U.S.C. §§ 2701–2712 (2012).

11. U.S. CONST. amend. IV.

12. WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a), at 575–76 (5th ed. 2012); *see* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that the Fourth Amendment is not violated "unless there has been . . . an actual physical invasion").

13. 389 U.S. 347 (1967).

14. *Id.* at 353 (holding that the government conducted an unreasonable search by using an electronic listening device attached to a public telephone booth to record the defendant's conversation).

In his concurring opinion in *Katz*, Justice John Marshall Harlan II articulated what has become the current two-prong standard for determining when a search occurs within the meaning of the Fourth Amendment.[15] A search occurs when the government's action violates an expectation of privacy that is both (1) actually (subjectively) held by an individual and (2) recognized by society as (objectively) reasonable.[16]

However, the Fourth Amendment protects only against "unreasonable" searches.[17] Warrantless searches are presumptively unreasonable.[18] Therefore, when the government violates an individual's reasonable expectation of privacy without a warrant, an unconstitutional search has occurred.[19]

Although *Katz* broadened the scope of the Fourth Amendment beyond physical intrusions, just how far its protections extend remains unclear.[20] The *Katz* standard does not "dictate what a reasonable expectation of privacy is."[21] Instead, it provides a framework for courts and judges to make this determination on a case-by-case basis.[22]

B. The Third-Party Doctrine

Although the *Katz* standard does not predict a specific result,[23] the Supreme Court clarified its analysis in the 1970s, crafting what has become known as the third-party doctrine. First, in *United States v. Miller*,[24] the government compelled two banks to disclose all records concerning any accounts in the defendant's name.[25] The defendant contended that the government's procurement of the records was a violation of his Fourth Amendment rights.[26] The Court, however, disagreed and concluded that the defendant lacked a reasonable expectation of privacy in the financial records.[27]

The Court first found that the records were not the defendant's "private papers."[28] Rather, the documents obtained were the "business records of the banks,"[29] as the information they contained was recorded and kept by the

15. *Id.* at 361 (Harlan, J., concurring).
16. *Id.*
17. U.S. CONST. amend. IV.
18. *See* Kentucky v. King, 563 U.S. 452, 459 (2011).
19. *See* Kyllo v. United States, 533 U.S. 27, 33 (2001).
20. LAFAVE, *supra* note 12, § 2.1(b), at 582; *see* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 252 (1993).
21. *See* Peter Winn, Katz *and the Origins of the "Reasonable Expectations of Privacy" Test*, 40 MCGEORGE L. REV. 1, 12 (2009).
22. *See id.*; *see also* Cloud, *supra* note 20, at 253 (explaining that the *Katz* standard allows judges to determine which privacy expectations are reasonable based on their own ideas).
23. *See* Winn, *supra* note 21, at 12.
24. 425 U.S. 435 (1976).
25. *Id.* at 437–38.
26. *Id.* at 442.
27. *Id.*
28. *Id.* at 440.
29. *Id.*

banks in the "ordinary course of business."[30] As a result, the Court found that the defendant did not have a legitimate expectation of privacy in the records' contents.[31]

The Court then explained that the Fourth Amendment does not prevent the government from obtaining "information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[32] Because the defendant voluntarily conveyed the information in the records to the banks, the government did not violate his Fourth Amendment rights by thereafter obtaining that information.[33]

Three years later, in *Smith v. Maryland*,[34] the Supreme Court reached a similar conclusion. In that case, the police requested that the defendant's phone company install a pen register device to record all of the numbers the defendant dialed from his home phone.[35] The government then obtained the list of numbers from the phone company and introduced it as evidence against the defendant in his trial for robbery.[36] As in *Miller*, the defendant contended that the government's actions violated his Fourth Amendment rights.[37]

Once again, however, the Court disagreed and mirrored its reasoning in *Miller* to find that the defendant lacked a reasonable expectation of privacy in the list of numbers. The Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[38] It explained that regardless of whether a pen register device is installed, telephone users know they reveal the numbers dialed from their phones to the phone company.[39] Thus, because the defendant "voluntarily conveyed" the numbers to the telephone company,[40] his privacy interest in the numbers did not satisfy the second prong of the *Katz* standard.[41]

Today, *Katz*, *Miller*, and *Smith* are the foundation of the third-party doctrine—that an individual does not have a reasonable expectation of privacy in information voluntarily revealed to third parties.[42] Because the individual's expectation of privacy fails the objective prong of the *Katz* test, the government does not conduct an unreasonable search by subsequently gathering that information.[43] Importantly, the methods of generating and recording information in CSLI records make the third-party doctrine particularly relevant in this context.

---

30. *Id.* at 442.
31. *See id.*
32. *Id.* at 443.
33. *See id.*
34. 442 U.S. 735 (1979).
35. *Id.* at 737.
36. *Id.* at 737–38.
37. *Id.*
38. *Id.* at 743–44.
39. *Id.* at 742.
40. *Id.* at 744.
41. *See id.* at 745.
42. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
43. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

C. The Technology Behind CSLI

As previously noted, CSLI refers to the information generated by the communication of a mobile phone and cell tower, or cell site, constructed by the phone's service provider. Anytime a cell phone is turned on, it sends out a radio signal that identifies the nearest tower with which the phone then "registers" to obtain service.[44] The registration process occurs each time the phone is used to communicate, such as through a phone call or text message.[45] However, even when the phone is not being used to communicate, the registration process occurs automatically every seven seconds, so long as the phone is powered on.[46] Therefore, the only way to prevent registration is to turn the phone off.[47]

As the phone moves from one tower to the next, it continues to register, and the signal strength fluctuates accordingly, as indicated by the signal icon on the phone.[48] Towers measure the signal strength and, thus, the relative location of the phone through two methods.[49] The first method, known as time difference of arrival (TDOA), approximates the distance between the cell phone and tower by calculating the amount of time it takes for the signal to travel between the two.[50] The second method, known as angle of arrival (AOA), determines a phone's position based on the angle at which its signal reaches the tower.[51] When three or more towers receive a signal from the phone, service providers can locate a phone even more precisely using "triangulation methods."[52] Triangulation uses information about the signal's strength and the angle at which it was received at each tower to "virtually pinpoint" the phone's location.[53]

The accuracy of the location data also depends on the number of, and distance between, cell towers in a given area.[54] As the number of towers in a given region increases, the geographic area that each tower services

---

44. Owsley, *supra* note 2, at 5.

45. *See* Shannon Jaeckel, Comment, *Cell Phone Location Tracking: Reforming the Standard to Reflect Modern Privacy Expectations*, 77 LA. L. REV. 143, 147 (2016); *see also* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 885 (2014) (discussing location data generated through the use of downloadable applications such as email, Facebook, or Twitter).

46. Owsley, *supra* note 2, at 5.

47. *See* Stephanie Lockwood, *Who Knows Where You've Been?: Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 309 (2004) (noting that once a phone is turned off, it no longer registers with a tower). *But see* Freiwald, *supra* note 1, at 705 (suggesting that "further active intervention" may be required to prevent registration).

48. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 127 (2012); *see also* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) (noting that a cell phone user sees her phone's signal strength fluctuate in accordance with the phone's location relative to the nearest tower).

49. *See* Lockwood, *supra* note 47, at 308.

50. *See id.* at 308–09.

51. *See id.* at 309.

52. Freiwald, *supra* note 1, at 712.

53. *Id.*

54. *See id.* at 710.

decreases.[55] In urban areas, cell towers are more concentrated to accommodate for increased communications.[56] In these areas, towers are typically placed within a few hundred feet of each other.[57] Thus, a phone's signal has to travel only a few hundred feet to reach the closest tower.[58] By contrast, in rural towns, towers can be located several miles apart.[59] As a result, a phone's signal must travel several miles before registering with the closest tower, diminishing the accuracy of the phone's location.[60]

At the same time registration occurs, however, the phone's service provider records the information used to generate the connection between the phone and the tower.[61] CSLI refers to the information contained in these records. In particular, at each registration, the service provider records which cell tower the phone registered with, which portion of the tower is facing the phone at that time, and how strong the signal is, which indicates the distance between the phone and tower at the time of registration.[62] While CSLI does not include the content of any particular communication,[63] it allows service providers to estimate the location of the phone within one hundred feet or less.[64]

Over a period of a time, CSLI allows the service provider to create a "virtual map."[65] This map is comprised of data points indicating where the phone's user has traveled and for how long.[66] As a result, service providers maintain a "virtually complete record of a customer's location at all times."[67]

CSLI records can be further divided into two categories: historical and prospective location data.[68] Historical CSLI allows police to determine the past locations of a cell phone using information from towers that the phone previously contacted.[69] Prospective, or real-time, CSLI permits police to determine the phone's current location as it registers with each tower.[70] However, prospective CSLI remains outside the scope of this Note, which addresses only the government's ability to obtain historical CSLI from service providers.[71] Significantly, though, at least one scholar found that

55. *See* Pell & Soghoian, *supra* note 48, at 127; *see also* David Oscar Markus & Nathan Freed Wessler, *That '70s Show: Why the 11th Circuit Was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case*, 70 U. MIAMI L. REV. 1179, 1183 (2016).

56. Freiwald, *supra* note 1, at 710.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. *See* Owsley, *supra* note 2, at 5.

62. *See id.*

63. R. Craig Curtis et al., *Using Technology the Founders Never Dreamed Of: Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 63 (2014).

64. Owsley, *supra* note 2, at 33.

65. Freiwald, *supra* note 1, at 705–06.

66. *See id.*

67. Henderson, *supra* note 4, at 806.

68. Curtis et al., *supra* note 63, at 63.

69. *See id.*

70. *See id.*

71. There is currently a debate over whether historical and prospective CSLI should be subject to the same legal analysis for Fourth Amendment purposes. *Compare* Curtis et al.,

many courts have "held that the Fourth Amendment requires a [search] warrant to obtain such forward-looking data."[72]

Nonetheless, law enforcement officials often seek to obtain historical CSLI from service providers during criminal investigations.[73] In many cases, police use this information to track a suspect's movements in relation to the scene of a recent crime.[74] Cell site data is particularly useful when investigating serial crimes such as robberies, assaults, and home invasions.[75] Not surprisingly, defendants often challenge the admissibility of this evidence on the ground that it was obtained in violation of their Fourth Amendment protections.[76] Courts considering these challenges, therefore, have had to determine whether and how the government may procure CSLI.[77]

D. The SCA and CSLI Disclosure

The SCA currently regulates the government's access to cell-phone-related records.[78] The statute divides communication information that the government seeks into two separate categories.[79] The first category, found under § 2703(a)–(b), includes the content of communications.[80] The second category, found under § 2703(c), includes the "records concerning electronic communication service or remote computing service."[81] Because CSLI does not include the content of any communication, "most courts . . . have assumed" it falls into the latter group.[82]

Under § 2703(c), the government may compel a service provider to disclose these "records" by obtaining (1) a search warrant supported by probable cause,[83] (2) consent of the customer for whom they seek the information,[84] or (3) a court order pursuant to § 2703(d).[85] In turn, § 2703(d) provides that a court order will be granted if the government offers "specific

---

supra note 63, at 89–91 (arguing for a uniform, probable cause standard for access to all CSLI), *and* Freiwald, *supra* note 1, at 738–40 (arguing that the historical nature of the location data should not change the legal analysis), *with* Pell & Soghoian, *supra* note 48, at 174–93 (proposing a statute that governs law enforcement's access to historical and prospective CSLI differently).

72. Freiwald, *supra* note 1, at 698–99.

73. *See* P. Kramer Rice, *You Are Here: Tracking Around the Fourth Amendment to Protect Smartphone Geolocation Information with the GPS Act*, 38 SETON HALL LEGIS. J. 17, 23–24 (2013); *see also* Pell & Soghoian, *supra* note 48, at 120–21.

74. *See, e.g.*, United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 501 (11th Cir. 2015).

75. *See* Owsley, *supra* note 2, at 6.

76. *See, e.g.*, *Graham*, 824 F.3d at 424; *Carpenter*, 819 F.3d at 885–86; *Davis*, 785 F.3d at 504.

77. *See infra* Part II.A.

78. 18 U.S.C. §§ 2701–2712 (2012).

79. *Id.* § 2703(a)–(c).

80. *Id.* § 2703(a)–(b).

81. *Id.* § 2703(c).

82. Freiwald, *supra* note 45, at 883. Some scholars, however, question the validity of this assumption. *See infra* Part II.B.4.

83. 18 U.S.C. § 2703(c)(1)(A).

84. *Id.* § 2703(c)(1)(C).

85. *Id.* § 2703(c)(1)(B).

and articulable facts showing that there are reasonable grounds to believe" the information sought is relevant to a current investigation.[86]

Importantly, the "specific and articulable facts" standard is less stringent than the probable cause standard required to obtain a search warrant.[87] As a result, the government often procures CSLI using a court order under § 2703(d), commonly referred to as a "'d' order,"[88] rather than a warrant.[89]

E. The Supreme Court and Government Surveillance

The Supreme Court has not yet addressed whether the warrantless procurement of CSLI, such as through the use of a "d order," violates the Fourth Amendment. However, the Court has decided similar cases involving technological surveillance by the government. These decisions inform the CSLI analysis.

First, in *United States v. Knotts*,[90] the government placed a beeper inside a chemical container, which the defendant then transported from Minnesota to Wisconsin by car.[91] The beeper emitted periodic radio signals, which the government picked up using a radio receiver.[92] This enabled the government to track the container and, thus, the defendant's location from one state to the next.[93] Before trial, the defendant moved to suppress the location information obtained through the beeper.[94]

The case eventually reached the Supreme Court, which held that the warrantless monitoring of the defendant's location did not violate his Fourth Amendment rights.[95] Because he "travelled over . . . public streets," the defendant "voluntarily conveyed" his location to anyone who looked his way.[96] As a result, the Court held that a person "traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[97]

---

86. *Id.* § 2703(d). *But see infra* note 191 and accompanying text (discussing the disagreement between the Third and Fifth Circuits over whether the language of § 2703(d) gives a court discretion to issue an order upon the government satisfying this standard).

87. *Historical Cell Site Data Case*, 724 F.3d 600, 606 (5th Cir. 2013); *In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 313 (3d Cir. 2010).

88. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219 (2004); *see* Freiwald, *supra* note 45, at 880–81.

89. *See, e.g.*, United States v. Graham, 824 F.3d 421, 426 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 502 (11th Cir. 2015); *Historical Cell Site Data Case*, 724 F.3d at 602; *In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 305; *see also* Steven M. Franklin, Comment, *Big Brother Is Watching You: Government Surveillance Through Cell-Site Location Information and the Fourth Circuit's Attempt to Stop It*, 51 WAKE FOREST L. REV. 493, 498 (2016).

90. 460 U.S. 276 (1983).

91. *Id.* at 277.

92. *Id.*

93. *Id.*

94. *Id.* at 279.

95. *Id.* at 285.

96. *Id.* at 281–82.

97. *Id.*

Second, in *United States v. Karo*,[98] the government again placed a beeper inside a chemical container, which was then used to locate the container inside of the defendant's home.[99] The Court held the government's warrantless monitoring violated the defendant's Fourth Amendment protections.[100] Distinguishing *Knotts*, the Court found the government gained information about the inside of the defendant's home that could not otherwise be visually verified.[101] As a result, the Court held that the warrantless monitoring of property within one's home, which is hidden from "public view," violates the privacy interests one has within his home.[102]

Lastly, in *United States v. Jones*,[103] the government installed a global positioning system (GPS) device on the defendant's car and tracked its movements for twenty-eight days.[104] Relying on the traditional trespass-based approach of the Fourth Amendment, the Court held that the government violated the defendant's Fourth Amendment rights because it "physically occupied private property" without a warrant to install the device.[105] However, five Justices wrote or joined concurring opinions analyzing the case under a different approach, focusing on the government's GPS surveillance rather than the trespass.

Justice Alito, writing for Justices Ginsburg, Breyer, and Kagan, wrote that "long[] term GPS monitoring in investigations of most offenses impinges on [one's] expectation[] of privacy."[106] Although he noted that short-term monitoring would not implicate the Fourth Amendment,[107] Justice Alito doubted that people expect law enforcement to trace an individual's movements over a long period of time.[108] Justice Alito did not specify at what point the monitoring becomes a search within the meaning of the Fourth Amendment.[109] However, he noted that "the line was surely crossed before the 4-week mark."[110]

Justice Sotomayor, writing alone, also focused on the government's use of GPS surveillance and framed the issue in the case under a similar approach.[111] Although she agreed with Justice Alito's concerns about long-term monitoring,[112] Justice Sotomayor wrote first that "even short-term monitoring" can be problematic.[113] She noted that GPS monitoring creates a "comprehensive record of a person's public movements that reflects a

98. 468 U.S. 705 (1984).
99. *Id.* at 708.
100. *Id.* at 714.
101. *Id.* at 715.
102. *Id.* at 716.
103. 132 S. Ct. 945 (2012).
104. *Id.* at 948.
105. *Id.* at 949.
106. *Id.* at 964 (Alito, J., concurring).
107. *See id.*
108. *See id.*
109. *See id.*
110. *Id.*
111. *See id.* at 954–57 (Sotomayor, J., concurring).
112. *Id.* at 955.
113. *Id.*

wealth of detail about her familial, political, professional, religious, and sexual associations."[114] Focusing on the "sum of one's public movements,"[115] she then stated that the proper inquiry is "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."[116]

Justice Sotomayor also questioned validity of the third-party doctrine.[117] She stated that the doctrine is "ill suited to the digital age,"[118] as people today reveal a vast amount of information about themselves to third parties in carrying out "mundane tasks."[119] In her view, information that has been disclosed to "some member of the public for a limited purpose" does not necessarily lose Fourth Amendment protection solely for that reason.[120]

Nonetheless, because *Jones* dealt with GPS devices and because the majority's holding was rooted in trespass, circuit courts have not applied *Jones* in the context of CSLI, where physical trespass is absent. And despite Justices Alito's and Sotomayor's concurring opinions, circuit courts have continually held that the warrantless procurement of CSLI is not a Fourth Amendment violation.[121] However, many scholars disagree with these decisions and support the opposite position using a number of different rationales.[122]

II. CSLI TRACKING: JUDICIAL OUTCOMES AND ACADEMIA'S RESPONSE

This part articulates the disagreement between the federal appellate judiciary and academia over the warrantless use of CSLI records.

A. Circuit Court Treatment of CSLI

As discussed, § 2703(c) of the SCA permits the government to obtain CSLI with a court order rather than a search warrant.[123] And because the "specific and articulable facts" standard required for such an order is less stringent than the probable cause standard required for a warrant,[124] the government commonly relies on this section to procure CSLI from service providers.[125]

114. *Id.*
115. *Id.* at 956.
116. *Id.*
117. *See id.* at 957.
118. *Id.*
119. *Id.* ("People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.").
120. *Id.*
121. *See infra* Part II.A.
122. *See infra* Part II.B.
123. 18 U.S.C. § 2703(c)(1)(B) (2012).
124. *Historical Cell Site Data Case*, 724 F.3d 600, 606 (5th Cir. 2013); *In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 313 (3d Cir. 2010).
125. *See supra* note 89 and accompanying text.

When defendants move to suppress this evidence on Fourth Amendment grounds, the central inquiry under *Katz* is whether mobile phone customers have a reasonable expectation of privacy in CSLI.[126]

To date, four of the five circuit courts to address this question have answered in the negative.[127] In these jurisdictions, therefore, the government may lawfully procure CSLI from service providers without a warrant. In support of their holdings, the circuit courts have relied primarily on two rationales. First, all of these circuit courts found that the third-party doctrine prevents individuals from maintaining a reasonable expectation of privacy in CSLI.[128] Second, most of these circuits also found that the data contained in CSLI is analogous to the business records kept by a private company, which are not subject to Fourth Amendment protections.[129]

1. Application of the Third-Party Doctrine

First, as noted, most of the circuits have used the third-party doctrine to conclude that mobile phone users do not have a reasonable expectation of privacy in CSLI. Recently, for example, in *United States v. Graham*,[130] the government procured CSLI for the defendants' cell phones for 221 days.[131] The government obtained the information through a court order under § 2703(d) of the SCA[132] and then used the CSLI to track the defendants' locations in relation to several robberies.[133]

At trial, the defendants moved to suppress the CSLI evidence.[134] The district court denied the motions,[135] and the defendants appealed to the Fourth Circuit, where a three-judge panel held that the government's warrantless procurement of CSLI was an unreasonable search under the

126. *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016).

127. *Id.* at 427; United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015); *Historical Cell Site Data Case*, 724 F.3d at 614–15. *But see In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 312, 319 (declining to address whether defendants maintained a reasonable expectation of privacy in CSLI, but holding that the government may not always be required to secure a warrant before obtaining it).

128. *See, e.g.*, *Graham*, 824 F.3d at 427; *Carpenter*, 819 F.3d at 889; *Davis*, 785 F.3d at 511; *Historical Cell Site Data Case*, 724 F.3d at 610–14.

129. *See, e.g.*, *Carpenter*, 819 F.3d at 885–86; *Historical Cell Site Data Case*, 724 F.3d at 611–12.

130. 824 F.3d 421 (4th Cir. 2016).

131. United States v. Graham, 796 F.3d 332, 341 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421.

132. *Id.* at 343.

133. *Id.* at 342–43.

134. *Id.* at 342.

135. *Id.*

Fourth Amendment.[136] However, after a rehearing en banc, the Fourth Circuit reversed the panel's decision.[137]

The court expressly held that "individuals do not have a reasonable expectation of privacy in . . . CSLI."[138] In support of its holding, the court noted that the third-party doctrine resolved any issues regarding the government's procurement of CSLI[139]: by using their cell phones, the defendants necessarily revealed their location to their third-party service provider, Sprint/Nextel.[140] Therefore, they could not claim a reasonable expectation of privacy in the information,[141] and the government was permitted to obtain the CSLI using only a court order.[142]

The Fourth Circuit found support for its application of the third-party doctrine to CSLI in its sister circuits' decisions.[143] In *United States v. Carpenter*,[144] for example, the Sixth Circuit confronted facts similar to those in *Graham*. In *Carpenter*, the government obtained a year's worth of CSLI, which was used to track the defendants' location in relation to a robbery and other related crimes.[145] The government compelled the defendants' service providers to disclose the information through a court order under § 2703(d).[146]

Relying on the third-party doctrine, the Sixth Circuit held that mobile phone users do not have a reasonable expectation of privacy in CSLI.[147] The court found that cell phone users knowingly expose their location to their service providers for at least two reasons.[148] First, most cell phone users have seen their phone's signal strength fluctuate through its signal icon.[149] Thus, users know that they are exposing their location to the nearest tower and the service provider that operates it.[150] Second, cell phone users know that they will be billed for "roaming" charges when they use their phone outside of the provider's network.[151] Thus, customers should know that service providers record their locational information.[152] As a result, the court held that cell

136. *Id.* at 343. Although the panel found that the warrantless procurement of CSLI violated the defendants' Fourth Amendment rights, it affirmed the district court's denial of the suppression motions on other grounds. *Id.* at 361, 363. Nonetheless, as the Fourth Circuit later noted en banc, the panel's holding instructed the government to first secure a search warrant before procuring CSLI from providers in the future. *Graham*, 824 F.3d at 424.

137. *Graham*, 824 F.3d at 424 (holding that "the Government's acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment").

138. *Id.* at 428.

139. *Id.* at 427.

140. *Id.*

141. *Id.* at 435–36.

142. *Id.* at 438.

143. *Id.* at 428 (noting that the Fifth, Sixth, and Eleventh Circuits have held that mobile phone users lack a reasonable expectation of privacy in CSLI).

144. 819 F.3d 880 (6th Cir. 2016).

145. *Id.* at 884.

146. *Id.* at 886.

147. *Id.* at 888.

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

phone users lack a reasonable expectation of privacy in CSLI because they knowingly expose their location to their service providers.[153]

The Fifth Circuit, in *In re Application of the United States for Historical Cell Site Data*,[154] took a position similar to that of the Fourth and Sixth Circuits. The court noted first that cell phone use is completely voluntarily on the part of the user.[155] Second, the court found that mobile phone customers "understand" that their location is being used by the service provider to deliver a signal to the customer's phone.[156] Therefore, the user's knowledge that their location will be revealed to their third-party provider precludes a claim of privacy in CSLI.[157] As a result, the court held that a warrant is not required to obtain it.[158]

2. The Business Record Analogy

Some circuits have considered not only the method of collecting CSLI but also the nature of the data it contains. The Sixth Circuit, for example, noted that the information contained in CSLI excludes the actual content of any communication.[159] Rather, the court found that CSLI merely represents the "information necessary to get those communications from point A to point B."[160] In doing so, the Sixth Circuit analogized CSLI to the business records discussed in *Miller* and *Smith*.[161] It found that CSLI was "created and maintained"[162] by the service provider for legitimate purposes.[163] While the Fourth Amendment protects the private contents of communications, individuals do not maintain a protected interest in the business records created by a company.[164] The government's subsequent gathering of that information is therefore not a violation of a cell phone user's privacy.[165]

The Eleventh Circuit also found this rationale persuasive. In *United States v. Davis*,[166] the government obtained CSLI for a period of sixty-seven days to trace the defendant's location in relation to series of seven robberies.[167] After the defendant was convicted, he appealed to the Eleventh Circuit.[168] A three-judge panel held that because the government obtained the data

153. *Id.*
154. 724 F.3d 600 (5th Cir. 2013).
155. *Id.* at 613 (noting that individuals are required neither to use cell phones nor to purchase service from a provider who maintains CSLI records).
156. *Id.*
157. *See id.* at 612–14.
158. *Id.* at 614.
159. United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016).
160. *Id.* at 886.
161. *See id.* at 887–89.
162. *Id.* at 888.
163. *Id.* at 887 (noting that service providers may keep CSLI records to improve weak spots in their network).
164. *Id.*; *see* United States v. Miller, 425 U.S. 435, 442–43 (1976).
165. *Carpenter*, 819 F.3d at 887 ("The government's collection of business records containing these [locational] data therefore is not a search.").
166. 785 F.3d 498 (11th Cir. 2015).
167. *Id.* at 501.
168. *Id.* at 504.

pursuant to a court order rather than a warrant, the defendant's Fourth Amendment rights were violated.[169] After a rehearing en banc, however, the Eleventh Circuit reversed the decision, holding that the defendant did not have a constitutionally protected privacy interest in CSLI.[170]

The court held that the defendant lacked a reasonable expectation of privacy in CSLI in part because the information constituted a business record of the service provider.[171] The court found that the CSLI records did not belong to the defendant, "even if [they] concern[ed] him."[172] Rather, the "records were created by [the service provider], stored on its own premises, and subject to its control."[173] The court further explained that CSLI excluded the "private communications" of the defendant and was used by the company only for legitimate business purposes.[174] Therefore, the defendant could not claim ownership of, or privacy in, the CSLI records.[175] As a result, the government was not required to obtain a warrant before compelling the service provider to disclose the locational information.[176]

3. The Third Circuit's Discretionary Standard

Although most circuits have based their holdings on the third-party doctrine, the Third Circuit declined to do so. Its holding in *In re Electronic Communication Service to Disclose*[177] departs from those of its sister circuits in a significant way. In that case, a magistrate judge denied the government's request for a court order compelling a service provider to disclose CSLI.[178] In doing so, the magistrate judge held that a cell phone is a "tracking device," which is not governed by the SCA.[179] Consequently, the government was required to show probable cause to obtain a search warrant before accessing the phone's locational information.[180]

On appeal, the Third Circuit rejected the government's argument that cell phone users lack a reasonable expectation of privacy in CSLI based on the third-party doctrine.[181] The court found that a "cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any

169. *Id.* at 504–05.
170. *Id.* at 500, 511.
171. *Id.* at 511.
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*
176. *See id.* at 518 (holding that the government only needed a court order pursuant to § 2703(d)). In addition to the Sixth and Eleventh Circuits, the Fifth Circuit also compared CSLI to a business record and similarly analyzed the information according to *Smith* and *Miller*. *Historical Cell Site Data Case*, 724 F.3d 600, 615 (5th Cir. 2013) ("Cell site data are business records and should be analyzed under that line of Supreme Court precedent.").
177. 620 F.3d 304 (3d Cir. 2010).
178. *Id.* at 305.
179. *Id.* at 309. Congress defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b) (2012). However, the SCA excludes communication from "tracking devices" from the types of "electronic communication" obtainable under § 2703(c). *Id.* § 2510(12)(C).
180. *In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 308.
181. *See id.* at 317–18.

meaningful way," as the customer is likely unaware that his provider collects such data.[182] Nevertheless, the court declined to directly address whether individuals maintain a privacy interest the location information.[183] Instead, the Third Circuit turned to the language of the SCA to determine whether a warrant was required to obtain it.

First, the court rejected the contention that a cell phone is a tracking device and, therefore, not covered by the SCA.[184] Rather, the court noted that § 2703(d) of SCA applies to CSLI because the information is derived from "wire communication,"[185] which is explicitly governed by the statute and accessible by the government with a court order.[186] Thus, it held that "CSLI . . . is obtainable under a § 2307(d) order," regardless of the third-party doctrine's effect and "that such an order does not require the traditional probable cause determination."[187]

However, the court then explained that a court order may not be sufficient in all circumstances and granted the magistrate judge discretion in determining whether a warrant should be required in a given case.[188] Section 2703(d) states that a "court order for disclosure . . . *may* be issued by any court that is a court of competent jurisdiction and *shall* issue *only if*" the "specific and articulable facts" standard is met.[189] The Third Circuit explained that the word "may" is the "language of permission"[190] and that the phrase "only if" is used to denote a necessary condition, not a sufficient one.[191] As a result, the court held that even if the government meets the "specific and articulable facts" standard required for a court order, the SCA "gives the [magistrate judge] the option to require a warrant showing probable cause."[192] Nonetheless, in remanding the case, the Third Circuit noted that although requiring a warrant is an available option, it should be "used sparingly because Congress also included the option of a § 2703(d) order."[193]

---

182. *Id.* at 317.

183. *Id.* at 312 (stating, "We see no need to decide that issue" in the present case).

184. *Id.* at 313.

185. *Id.* at 310.

186. 18 U.S.C. § 2703(c) (2012). This section provides that the government may require the provider of an "electronic communication service" to disclose records or other information pertaining to a customer when it is has obtained the consent of the customer, a warrant supported by probable cause, or a court order under § 2703(d). *Id.* An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive *wire . . . communications*." *Id.* § 2510(15) (emphasis added). Finally, a "wire communication" is defined as "any aural transfer made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection." *Id.* § 2510(1).

187. *In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 313.

188. *Id.* at 319.

189. 18 U.S.C. § 2703(d) (emphasis added).

190. *In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 315.

191. *Id.* at 316. *But see Historical Cell Site Data Case*, 724 F.3d 600, 607 (5th Cir. 2013) (finding that the Third Circuit's interpretation ignored the use of the word "shall," which is the language of command directing a court to issue the order upon the proper showing).

192. *In re Elec. Commc'n Serv. to Disclose*, 620 F.3d at 319.

193. *Id.* Perhaps unsurprisingly, as one scholar notes, this instruction has left "magistrate judges largely in the dark about how to proceed." Freiwald, *supra* note 45, at 889.

B. Academic Treatment of CSLI

As the circuit courts have ruled on CSLI-related cases, scholars and students have tracked this issue and analyzed the courts' decisions.[194] Significantly, this scholarship clashes with the circuit courts' holdings, as many commentators argue that cell phone users do, in fact, have a reasonable expectation of privacy in CSLI.[195] In support of this conclusion, they contend that the third-party doctrine is inapplicable to locational data,[196] reject the proposition that CSLI is merely a business record,[197] and even question whether § 2703(c) of the SCA governs cell phone location data at all.[198]

1. A Reasonable Expectation of Privacy in CSLI

On a fundamental level, many scholars and commentators disagree with the notion that mobile phone customers lack a reasonable expectation of privacy in CSLI.[199] To the contrary, cell phone users maintain "both a subjective and an objective expectation of privacy" in location data, satisfying the *Katz* standard and rendering the government's warrantless procurement of CSLI an unreasonable search.[200]

First, as to the subjective prong, CSLI reveals a "large amount of sensitive and private information about a person's movements and activities in public and private spaces."[201] However, people "regard access to their location data as yielding private data"[202] and would be "unpleasantly surprised, if not outraged to learn" that the government could freely obtain their location information without a warrant.[203] Thus, cell phone users "surely entertain a subjective expectation of privacy" in CSLI.[204]

Second, the objective prong of *Katz* is also satisfied, as "Americans have a *reasonable* expectation of privacy in their cell phone records" as well.[205]

194. *See generally* Dennis J. Braithwaite & Allison L. Eiselen, *Nowhere to Hide?: An Approach to Protecting Reasonable Expectations of Privacy in Cell Phone Location Data Through the Warrant Requirement*, 38 AM. J. TRIAL ADVOC. 287 (2014); Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215 (2015); Curtis et al., *supra* note 63; Freiwald, *supra* note 1; Markus & Wessler, *supra* note 55; Franklin, *supra* note 89; Robert Harrington, Note, *Avoiding Scylla and Charybdis: Why the Third Party Doctrine Is Ill Suited to Treat CSLI, and What the State Courts Can Do About It*, 4 VA. J. CRIM. L. 361 (2016).

195. *See infra* notes 199–08 and accompanying text.

196. *See infra* notes 209–19 and accompanying text.

197. *See infra* notes 220–28 and accompanying text.

198. *See infra* notes 229–40 and accompanying text.

199. *See, e.g.*, Curtis et al., *supra* note 63, at 90 (arguing that a reasonable expectation of privacy in cell phone records is consistent with Fourth Amendment values); Freiwald, *supra* note 1, at 743–46 (discussing individuals' subjective and objective expectations of privacy in CSLI); Markus & Wessler, *supra* note 55, at 1204 (contending that "CSLI data . . . violates reasonable expectations of privacy").

200. Lockwood, *supra* note 47, at 315.

201. Markus & Wessler, *supra* note 55, at 1204.

202. Freiwald, *supra* note 1, at 744.

203. *Id.* at 743.

204. *Id.* at 744.

205. Curtis et al., *supra* note 63, at 90 (emphasis added).

Generally, people do not expect their locations and movements to be monitored by the government through their cell phones.[206] And because cell phones play a "vital role" in today's era of private communication,[207] denying Fourth Amendment protection to location data ignores the "set of expectations that Americans have" with respect to this information.[208]

2. The Third-Party Doctrine Does Not Apply

Equally important, scholars further argue that the third-party doctrine is inapplicable to CSLI and does not diminish or eliminate a cell phone user's reasonable expectation of privacy in their location data.[209] First, mobile phone customers do not "voluntarily" convey their location to service providers.[210] Because registration automatically occurs every seven seconds, users do not enter locational information into their phones—as the defendant in *Smith* had done with the numbers he dialed—nor otherwise "affirmatively transmit[]" their location to the service provider.[211] Rather, the only affirmative action on the part of the user is buying the phone, as CSLI is an automatically generated byproduct.[212] Therefore, cell phone users could only "voluntarily" reveal their location if they understood the mechanics of CSLI prior to buying the phone.[213]

However, most cell phone users simply lack this knowledge.[214] Although service providers may include information about CSLI in their contracts, customers rarely read these agreements, and even if they do, it is likely not in an effort to find a CSLI-related provision.[215]

Moreover, even assuming that cell phone users are aware of registration and the resulting CSLI, they remain unable to prevent disclosing their location to service providers.[216] Today, cell phones are a ubiquitous part of society.[217] Family members, friends, and employers all require us to carry and use them, making it "very hard in today's world to exist without a cell phone."[218] As a result, they have become necessary in the modern era and refusing to own a phone or keeping one turned off at all times to avoid location disclosure is not practical.[219]

---

206. *See* Lockwood, *supra* note 47, at 316.
207. Freiwald, *supra* note 1, at 745; *see* Curtis et al., *supra* note 63, at 90.
208. Curtis et al., *supra* note 63, at 90.
209. *See, e.g.*, Freiwald, *supra* note 1, at 735–38; Markus & Wessler, *supra* note 55, at 1203; Harrington, *supra* note 194, at 380–84; *see also* Braithwaite & Eiselen, *supra* note 194, at 303–06.
210. *See* Freiwald, *supra* note 1, at 735–38; Markus & Wessler, *supra* note 55, at 1202–03; Harrington, *supra* note 194, at 381–88; *see also* Braithwaite & Eiselen, *supra* note 194, at 299.
211. Markus & Wessler, *supra* note 55, at 1203.
212. Freiwald, *supra* note 1, at 736.
213. Harrington, *supra* note 194, at 382.
214. Freiwald, *supra* note 1, at 737; *see* Curtis et al., *supra* note 63, at 63 ("Most people are not aware of just how much data cell phone companies are storing and for how long.").
215. Curtis et al., *supra* note 63, at 90.
216. *See* Harrington, *supra* note 194, at 383–84.
217. *See* Markus & Wessler, *supra* note 55, at 1193.
218. Curtis et al., *supra* note 63, at 90.
219. *See* Pell & Soghoian, *supra* note 48, at 126; Harrington, *supra* note 194, at 383.

3. CSLI Is Not a Business Record

In addition to criticizing the third-party doctrine, commentators have also attacked the proposition that CSLI is merely a record kept by the service provider in the ordinary course of business.[220] At least one scholar suggests that when the government compels service providers to disclose CSLI, the providers do not produce anything that resembles a routine business record.[221] Rather, the documents disclosed look more like either "customized report[s]" tailored to the government's request or, on the other end of the spectrum, "raw data."[222] In either case, the documents produced during CSLI disclosure hardly look like information that would be regularly kept or presented to a customer.[223]

In addition to the records' form, the nature of the data contained in CSLI also "needs to be addressed,"[224] as this information should not be treated like ordinary business records.[225] CSLI provides detailed information about people's communication, movements, and activities—disclosing more personal information, such as where users go and how long they spend there, than the banking records in *Miller*.[226] Because CSLI reveals this "large amount of sensitive and private information,"[227] it more closely resembles the private communications that were protected by the Fourth Amendment in *Miller* than the financial information that was not.[228]

4. Section 2703(c) Does Not Govern CSLI

Lastly, some commentators have also questioned whether § 2703(c) of the SCA governs CSLI at all.[229] Congress defines a mobile "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[230] Because a cell phone creates a record of its user's movements through CSLI, "[i]t makes sense to view a cell phone as a tracking device."[231] However, while § 2703(c) covers information relating to "electronic communication services,"[232] the SCA explicitly excludes "tracking device[s]" from its definition of "electronic

220. *See, e.g.*, Curtis et al., *supra* note 63, at 89–90; Freiwald, *supra* note 1, at 733–35; *see also* Markus & Wessler, *supra* note 55, at 1204–05.
221. *See* Freiwald, *supra* note 1, at 733–34.
222. *Id.* at 734.
223. *See id.*
224. Curtis et al., *supra* note 63, at 89.
225. Freiwald, *supra* note 1, at 734–35.
226. *See* Markus & Wessler, *supra* note 55, at 1203; *see also* Freiwald, *supra* note 1, at 734.
227. Markus & Wessler, *supra* note 55, at 1204.
228. *See* Freiwald, *supra* note 1, at 734.
229. *See* Freiwald, *supra* note 45, at 883–86.
230. 18 U.S.C. § 3117(b) (2012).
231. Freiwald, *supra* note 45, at 884.
232. 18 U.S.C. § 2703(c).

communication."[233] Thus, cell phones "should be excluded from the scope of records" obtainable under § 2703(c).[234]

Moreover, even if "tracking devices" were included within the SCA's definition of "electronic communication," they could still fall outside the scope of § 2703(c).[235] This section does not govern the content of any particular communication, as the government may obtain the "contents of . . . electronic communications" only under § 2703(a).[236] As one scholar notes, "The question is, what counts as contents, and what counts as noncontent" information?[237] In answering this question, however, a "judge could view location data as content information" and therefore obtainable only under § 2703(a), not § 2703(c).[238]

As a result, courts could construe location records to fall outside the scope of § 2703(c) by either viewing cell phones as tracking devices or location records as content information.[239] In either case, the government would be required to obtain a warrant before procuring a cell phone's locational records.[240]

C. Protection of CSLI Records

The discourse surrounding CSLI not only scrutinizes the circuit courts' decisions but also further advocates for the protection of cell phone location data under the Fourth Amendment. Notably, however, scholars do not agree on the extent and nature of that protection and which governmental institution is best suited to implement it.

1. Judicial Intervention and the Warrant Requirement

Because many scholars contend that individuals maintain a reasonable expectation of privacy in CSLI,[241] they also argue that the judiciary should require the government to obtain a search warrant before procuring this data from service providers.[242] Given the "accuracy and precision" with which CSLI can locate criminal suspects,[243] a warrant requirement affords innocent Americans protections against overreaching law enforcement activity.[244] And because the technology continues to develop at a rapid pace,[245] making

233. *Id.* § 2510(12)(C).
234. Freiwald, *supra* note 45, at 884.
235. *See id.* at 885.
236. 18 U.S.C. § 2703(a).
237. Kerr, *supra* note 88, at 1228.
238. Freiwald, *supra* note 45, at 885.
239. *See id.*
240. *See id.*
241. *See supra* Part II.B.1–3.
242. *See* Freiwald, *supra* note 1, at 748; Markus & Wessler, *supra* note 55, at 1191, 1195; *see also* Curtis et al., *supra* note 63, at 89–91.
243. Harrington, *supra* note 194, at 392; *see* Freiwald, *supra* note 1, at 724–25 (discussing how CSLI can even permit police to ascertain when an individual is in his own home).
244. Freiwald, *supra* note 1, at 726 (arguing that the "richness and precision" of CSLI and the likelihood that law enforcement will overcollect data mandates a warrant protection).
245. *See* Braithwaite & Eiselen, *supra* note 194, at 315.

it easier for the government to obtain a person's information, the law must respond accordingly by heightening the Fourth Amendment's protections.[246]

However, because the federal appellate courts have not yet held that a warrant is necessary, some commentators suggest that state courts should implement the requirement.[247] Although a decision from the Supreme Court or circuit courts would be "preferential,"[248] state courts are in a unique position to address the problem because they can act as "laboratories in the constantly changing world of technology."[249]

The Fourth Amendment acts as a "constitutional floor," establishing the minimum level of protection states must provide to their citizens.[250] However, each state has an "analog" to the Fourth Amendment of the U.S. Constitution.[251] State courts, therefore, are free to interpret their constitutional provisions to accord greater protection to individual rights than do the provisions of the federal Constitution.[252] For example, the Supreme Court of New Jersey held that cell phone users have a reasonable expectation of privacy in CSLI, forcing police to obtain a warrant before procuring location data from providers.[253] While few states have followed New Jersey's lead,[254] one scholar argues that the New Jersey Supreme Court's holding was "correct" and urges others to follow accordingly.[255]

2. Legislative Solutions and the SCA

Although a judge may impose a warrant requirement, some commentators argue for a legislative resolution to warrantless CSLI disclosure.[256] For example, some scholars contend that Congress or state legislatures should enact a statutory warrant requirement for all CSLI requests by the

246. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

247. *See, e.g.*, Braithwaite & Eiselen, *supra* note 194, at 308–14; Corbett, *supra* note 194, at 228; Harrington, *supra* note 194, at 394–99.

248. Curtis et al., *supra* note 63, at 91 (noting that the Supreme Court's interpretation of the Fourth Amendment has more "staying power"); *see* Markus & Wessler, *supra* note 55, at 1195 ("It is becoming increasingly urgent that the [Supreme] Court provide a clear . . . rule governing location data and other sensitive digital records.").

249. Braithwaite & Eiselen, *supra* note 194, at 288.

250. Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 374 (2006).

251. *Id.*

252. *Id.*; *see* Corbett, *supra* note 194, at 228.

253. State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

254. *See, e.g.*, Commonwealth v. Augustine, 4 N.E.3d 846, 849 (Mass. 2014); Commonwealth v. Rushing, 71 A.3d 939, 962–63 (Pa. Super. Ct. 2013), *rev'd on other grounds*, 99 A.3d 416 (Pa. 2014).

255. Braithwaite & Eiselen, *supra* note 194, at 308.

256. *See, e.g.*, Lockwood, *supra* note 47, at 317; Pell & Soghoian, *supra* note 48, at 180–81; Rice, *supra* note 73, at 31–32; *see also* Corbett, *supra* note 194, at 227–28.

government,[257] while others suggest the SCA's standard for a court order should be amended.[258]

The latter approach, proposed by two scholars, permits the government to compel a service provider to disclose historical CSLI using only a court order.[259] However, to obtain the order, the government must satisfy two requirements.[260] First, it must demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that the location information requested is relevant and material to an ongoing criminal investigation."[261] Second, the government must also demonstrate "specific and articulable facts showing that a reasonable and sufficient nexus exists between the alleged or suspected criminal activity . . . and the scope of the location data requested."[262]

To be clear, the authors did not propose a warrant requirement for historical CSLI disclosure. However, they hoped that requiring the government to justify the scope of its request properly weighed the privacy interest of mobile phone users without unduly limiting the police's ability to investigate suspected criminal activity.[263]

3. A Mosaic Approach to CSLI Protection

Finally, some commentators suggest that the "mosaic theory" of the Fourth Amendment should serve as the basis of protection for CSLI.[264] Generally, the mosaic theory proposes that courts "apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps."[265] More specifically, rather than considering whether a particular governmental act is a search, the theory focuses on whether a series of acts together constitutes a search.[266] Thus, "premised on aggregation," it asks

257. *See, e.g.*, Corbett, *supra* note 194, at 227–28 (explaining that state legislatures are free to pass laws requiring police to obtain a warrant before procuring CSLI from service providers); Lockwood, *supra* note 47, at 317 (urging legislators enact specific warrant requirements for cell phone data); Rice, *supra* note 73, at 31–32 (arguing for federal legislation that "effectively elevate[s] mobile phone CSLI . . . to the probable cause standard" required for a search warrant).

258. *See* Pell & Soghoian, *supra* note 48, at 180–81 (proposing an amendment to the SCA that includes a conjunctive two-prong standard for court orders).

259. *Id.* at 180.

260. *Id.*

261. *Id.*

262. *Id.* Absent a court order, the proposal permits a service provider to disclose locational data with the consent of the customer or as otherwise currently provided in 18 U.S.C. § 2702(c)(3)–(6) (2012). Pell & Soghoian, *supra* note 48, at 180.

263. Pell & Soghoian, *supra* note 48, at 181.

264. *See, e.g.*, Lance H. Selva et al., *Rise of the Mosaic Theory: Implications for Cell Site Location Tracking by Law Enforcement*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 235 (2016); *see also* Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard, *the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2011); Justin P. Webb, Note, *Car-ving Out Notions of Privacy: The Impact of GPS Tracking and Why* Maynard *Is a Move in the Right Direction*, 95 MARQ. L. REV. 751 (2011).

265. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).

266. *Id.*

"whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic" about the targeted individual's life.[267] Before turning to theory's application to CSLI, however, it is helpful to consider again the opinions in *Jones*, from which the mosaic theory stems.[268]

In *Jones*, the government physically placed a GPS tracking device on the defendant's car and used it to monitor the vehicle's location over twenty-eight days.[269] Although the majority resolved the case on trespass grounds,[270] Justices Alito and Sotomayor analyzed the case on a different basis, focusing on the government's use of GPS surveillance. Justice Alito stated that because people do not expect law enforcement to track an individual's movements over an extended period of time, long-term monitoring "impinges on [one's] expectations of privacy."[271] He then added that although the government monitored the defendant's location for twenty-eight days, the surveillance transformed into a search at some point "before the 4-week mark."[272] Thus, importantly, Justice Alito's opinion considers the amount or period of time over which the government's conduct persists, "which is critical to the mosaic approach."[273]

Similarly, Justice Sotomayor's concurrence also "clearly echoes the mosaic theory."[274] She suggested that, in cases of GPS monitoring, the proper inquiry focuses on the "sum of one's public movements."[275] Justice Sotomayor then stated that, in the context of government surveillance, the analysis should 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."[276] Although she agreed with Justice Alito's concern about long-term monitoring, she suggested that even short-term surveillance may be troublesome, depending on the amount of information the police are able to gather about the individual from the "sum" of their movements.[277]

Taken together, Justices Alito's and Sotomayor's opinions "create" the mosaic theory.[278] They focus on the "collective sum of government action," including the amount of time over which the government acts as well as the

267. *Id.*

268. *Id.* In fact, the theory was first considered in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2012), which was subsequently reviewed by the Supreme Court under the name *United States v. Jones*, 132 S. Ct. 945 (2012). Kerr, *supra* note 265, at 320.

269. *Jones*, 132 S. Ct. at 948.

270. *Id.* at 949 (holding that the government violated the defendant's Fourth Amendment rights because it "physically occupied private property" without a warrant when it installed the device on the defendant's car).

271. *Id.* at 964 (Alito, J., concurring).

272. *Id.*

273. Kerr, *supra* note 265, at 327.

274. *Id.* at 328.

275. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

276. *Id.*

277. *Id.* at 955.

278. Curtis et al., *supra* note 63, at 74.

amount and nature of the information it gathers, rather than on the government's individual actions or singular pieces of data they obtain.[279]

As noted, some commentators suggest that courts apply the mosaic approach when considering law enforcement's ability to obtain CSLI from service providers.[280] As a "more efficient and cost-effective" method of surveillance, "CSLI reveals more about a person" than GPS tracking because "people carry their cell phones wherever they go: in purses and pockets, to the doctor's office, to a political gathering, in their own home, and even inside their bedroom."[281] Thus, CSLI generates a wealth of information that has never before been available in one place to law enforcement officials.[282]

As a result, law enforcement's "[l]ong-term, continuous monitoring of cell site location information . . . fall[s] squarely within the contours of the mosaic theory."[283] As Justices Alito and Sotomayor suggested, society would not expect the police to covertly track and aggregate a person's every movement for long periods of time.[284] Because CSLI permits this kind of surveillance, cell site location tracking calls for Fourth Amendment protection.[285]

However, while the mosaic theory may be one of the "most compelling approach[es]" to address government surveillance,[286] some scholars have pointed out the practical problems that arise when trying to implement it.[287] In particular, Professor Orin S. Kerr thoughtfully details at least four issues that courts will need to address in order to administer the approach.[288]

The "first question concerns the standard that would govern the mosaic theory."[289] Courts will have to articulate what "test determines when a mosaic has been created."[290] Otherwise stated, courts will have to develop a standard for determining at what point the government's action gathers enough information about an individual such that their Fourth Amendment rights have been implicated.[291] Moreover, in developing this standard, courts will also have to determine which "stages of surveillance a mosaic search" includes.[292] Under this theory, it is unclear whether the government could

279. Kerr, *supra* note 265, at 328.
280. *See supra* note 264 and accompanying text.
281. Selva et al., *supra* note 264, at 255.
282. *Id.*
283. *Id.*
284. *See id.*
285. *Id.*
286. *Id.* at 256.
287. *See, e.g.*, Henderson, *supra* note 4, at 823–25 (analyzing the "administrability" of the mosaic theory); Kerr, *supra* note 265, at 328–43 (describing the challenges that come with implementing the mosaic approach).
288. Kerr, *supra* note 265, at 329–30.
289. *Id.* at 329.
290. *Id.*
291. *See id.* at 330–31 (arguing that the opinions from *Maynard* and *Jones* suggest three different standards for making this determination, all of which present their own issues of viability).
292. *Id.* at 329.

satisfy this standard simply by collecting data or whether "subsequent analysis and use" of that data would also be required.[293]

The second issue that arises when implementing the mosaic theory is a "grouping question."[294] Because the theory considers the "collective whole" of government conduct, courts will need to determine which conduct, or types of conduct, should be "grouped" together when evaluating whether that conduct poses a Fourth Amendment issue.[295] In turn, this will force courts to address several items, including which types of surveillance methods prompt the mosaic approach (e.g., GPS or CSLI tracking),[296] how long a specific tool or method of surveillance must be used before the mosaic theory is implicated,[297] and how different methods of surveillance used in one case should be grouped together, if at all, in determining whether a mosaic has been created.[298]

The third issue that the theory presents is how courts will "analyze the reasonableness of mosaic searches."[299] Because "each mosaic will be different," courts will have to develop a "framework" for determining the reasonableness of the government's action once it has been determined that a mosaic has been created.[300] For example, given the public/private distinction created by *Knotts* and *Karo*, courts will have to address whether public places will be treated differently than private areas, such as the home, or whether all locations in the mosaic will be treated "cumulatively."[301] Moreover, because mosaics can be created by different methods of surveillance, courts will be forced to decide whether one standard should be used for mosaics created by all methods of surveillance or whether the standard should be different for each method.[302]

The last issue that arises when adopting the mosaic theory concerns what "remedies" will apply for Fourth Amendment violations.[303] After determining that the government has violated an individual's Fourth Amendment rights under this theory, courts will then have to decide what recourse, if any, is available to the aggrieved party.[304] This will require courts to decide whether the exclusionary rule applies[305] and whether all of

293. *Id.* at 331–32 (explaining that while generally Fourth Amendment law considers only the acquisition of information, the mosaic theory may shift this focus because the "aggregation" principle suggests that "analysis" is required to create the mosaic).

294. *Id.* at 329.

295. *Id.*

296. *Id.*

297. *Id.* at 333.

298. *Id.* at 335–36 (noting also that courts will be forced to address whether the *same conduct* (for example, CSLI tracking) done by *different actors* (for example, state and federal law enforcement) should be grouped together for purposes of creating the mosaic).

299. *Id.* at 329.

300. *Id.*

301. *Id.* at 337.

302. *See id.* at 338.

303. *Id.* at 329–30.

304. *See id.*

305. Under traditional Fourth Amendment law, the exclusionary rule prevents the government from introducing evidence against a defendant that was obtained in violation of his Fourth Amendment rights. *Id.* at 340.

the information gathered by the police will be subject to the rule or only the information gathered after the point at which the court decides the mosaic was created.[306] Inevitably, courts will also likely confront situations wherein exceptions to the exclusionary rule may be appropriate and, therefore, must carefully articulate the scope and application of these exceptions.[307] Finally, courts will also have to consider whether, and under what circumstances, civil remedies may be available to the aggrieved party as well.[308]

Despite these obstacles, Kerr acknowledges that the mosaic theory "is animated by legitimate concerns."[309] However, he maintains that "courts should reject the mosaic theory" because "[it] would be very difficult to administer" given the aforementioned issues.[310] Moreover, despite having confidence in the judiciary to resolve these issues, Kerr notes that the challenges to the theory's implementation are emphasized by the lack of expert "opinion on how to apply it."[311]

III. THE MOSAIC THEORY AND WARRANTLESS CSLI MONITORING

This part aims to reconcile the competing arguments in the debate over warrantless CSLI monitoring by suggesting that courts analyze this information under the mosaic theory. This part first joins those who advocate for the theory's adoption and explains why this approach is best suited to address the underlying concerns with CSLI tracking. It then adds to the discussion by proposing a standard under which courts may apply the mosaic theory to CSLI.

A. The Mosaic Theory and the Problem with CSLI Tracking

The mosaic theory of the Fourth Amendment should be applied in the context of CSLI because it properly addresses the underlying concerns with the government's use of cell site locational data. Before the mosaic approach can be understood as the appropriate theory to analyze CSLI, however, it is necessary to see why both the trespass-based approach and the reasonable expectation of privacy test are insufficient to protect the interests at stake.

The Supreme Court made clear that the reasonable expectation of privacy test did not replace the trespass-based approach of the Fourth Amendment; it merely added to it.[312] As previously discussed, under the latter approach, the Fourth Amendment protects against physical intrusions upon one's body or property, such as their house, office, and automobile.[313] By definition, this approach is inapplicable in cases without physical trespass—such as the

306. *See id.* at 329–30.
307. *See id.*
308. *See id.*
309. *Id.* at 315.
310. *Id.*
311. *Id.* at 346–47.
312. United States v. Jones, 132 S. Ct. 945, 952 (2012).
313. LAFAVE, *supra* note 12, § 2.1(a), at 575; *see also supra* Part I.A.

government's procurement of CSLI—which the *Jones* Court conceded "would *remain* subject to *Katz* analysis."[314]

However, the *Katz* standard likewise fails to provide an appropriate framework for evaluating CSLI disclosure. The *Katz* Court held that the "Fourth Amendment protects people, not *places*."[315] On one level, the argument that CSLI should be protected under this standard undermines this holding to the extent that it effectively asks the Fourth Amendment to protect the *locations* contained in cell site *location* information. Admittedly, however, this conclusion ignores *Katz*'s idea that it is the individual's expectation of privacy within certain places, such as the level of privacy one expects to maintain within their home, that aggrieved parties seek to protect under the Fourth Amendment. Yet, this idea still does not address the underlying problems of CSLI monitoring.

The concern with CSLI tracking is not that individuals expect—or expect to maintain—privacy in certain locations. Rather, the concern stems from what one's presence at a given location can reveal about the details and activities of their daily personal life. As one scholar writes, location data permits law enforcement to "draw inferences about the substantive nature of the target's behavior based upon patterns revealed in the data."[316] Not surprisingly, the "more data that is available, the more inferences can be drawn to create a complete portrait of the subject's private life."[317] For example, as another scholar notes, CSLI can "reveal" or "divulge" when an individual has sought medical treatment, visited an abortion clinic, watched an X-rated movie, or protested at a political rally.[318]

However, while it stretches at least some standards of reasonableness to argue that people expect as much "privacy" at a movie theater or public rally as they do in their homes, it is easier to understand that people simply may not want the government monitoring their personal activities. The revealing nature of location data threatens an individual's more basic "right to be let alone,"[319] which "often ha[s] nothing to do with privacy at all."[320] Thus, the concerns about CSLI are based not necessarily on where individuals have been but rather on the government's ability to learn the more intimate details about who they are and what they are doing.

The mosaic theory of the Fourth Amendment is best suited to address these issues because it is concerned with the extent to which the government can "learn about a person's private affairs."[321] As Justice Sotomayor suggested in *Jones*, the analysis should focus on 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

314. *Jones*, 132 S. Ct. at 953.
315. United States v. Katz, 389 U.S. 347, 351 (1967) (emphasis added).
316. Braithwaite & Eiselen, *supra* note 194, at 302.
317. *Id.*
318. Freiwald, *supra* note 1, at 743.
319. *Katz*, 389 U.S. at 350.
320. *Id.*
321. Kerr, *supra* note 265, at 328.

beliefs, sexual habits, and so on."[322] Concerned with "individual liberties and freedoms,"[323] she feared that "[a]wareness that the Government may be watching"[324] would restrict the "associational and expressive freedoms"[325] people enjoy through their personal activities.

This Note, therefore, suggests that the mosaic theory is able to reconcile at least some of the competing arguments in the debate over warrantless CSLI procurement. On one hand, the circuit courts may have been correct to deny CSLI Fourth Amendment protection under the *Katz* standard. However, this Note does not suggest that these decisions were correct because of their reliance on the third-party doctrine and business record analogy. Rather, they are correct to the extent that the *Katz* standard is an inappropriate framework under which to properly analyze mobile phone users' concerns with CSLI surveillance. On the other hand, the mosaic theory can still provide those who advocate for constitutional protection of CSLI with an approach to achieve that goal, along with five Justices who may be ready to embrace it.[326]

B. The Mosaic Analysis

Indeed, the five votes that Justices Alito's and Sotomayor's concurrences received suggest the Supreme Court may be on the verge of changing its Fourth Amendment jurisprudence by adopting the mosaic theory. These votes, along with support for the theory among scholars and students, may also encourage lower courts to apply this approach before the Supreme Court has a chance to make such a change. However, courts choosing to do so will need to address the practical challenges that the theory poses as well as balance the government's interest in investigating criminal activity.

This Note creates a framework under which courts could apply the mosaic theory to CSLI by offering a resolution to two of the issues that arise in the theory's administration. First, this Note contends that CSLI monitoring should be a method of government surveillance subject to mosaic analysis.[327] Second, this Note offers a standard for determining whether the CSLI records obtained constitute a "search" within the meaning of the Fourth Amendment.[328] Importantly, this Note recognizes the difficulty in resolving these issues, as well as the others carefully outlined by Professor Kerr,[329] and it does not purport to provide a method by which the mosaic theory is seamlessly implanted into existing Fourth Amendment jurisprudence.

---

322. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
323. Selva et al., *supra* note 264, at 252.
324. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
325. *Id.*
326. In *Jones*, Justice Sotomayor wrote for herself, *id.* at 954, while Justice Alito was joined by Justices Ginsburg, Breyer, and Kagan, *id.* at 957 (Alito, J., concurring).
327. *See* Kerr, *supra* note 265, at 329, 334 (noting that administration of the mosaic theory will require courts to determine which methods of government surveillance would be subject to a mosaic analysis).
328. *See id.* at 329 (suggesting that courts will have to develop a standard to determine at what point a mosaic has been created).
329. *See supra* Part II.C.3.

Nonetheless, it does more than argue that the mosaic theory *should* be applied to CSLI: it also proposes a standard for *how* the theory may be applied.

The first issue to consider is the types or methods of surveillance that would be subject to a mosaic analysis. As stated above, the mosaic theory should apply to warrantless CSLI monitoring because of the amount of information it can reveal, the length of time over which it can be used, and its inexpensive cost to the government—features similar to those of the GPS tracking device in *Jones*.[330] Importantly, Justice Sotomayor noted that these features "require[d] particular attention"[331] before articulating the standard under which she would analyze government surveillance.[332] Furthermore, cell site location data can be easily aggregated over extended periods of time, such as over a 221-day period.[333] As a result, CSLI has the potential to offer information about an individual that as a whole is "more revealing" than the individual data points it consists of, placing cell phone location data appropriately within the confines of the mosaic theory.[334] Therefore, in cases where law enforcement officers procure and use CSLI without a warrant, the constitutionality of their conduct should be subject to a mosaic analysis.

Other methods of surveillance that share these attributes, improve upon them, or add to them may also be appropriate to analyze under the mosaic theory. While this Note does not endeavor to compare the methods of surveillance available to and used by law enforcement, courts implementing the mosaic theory will have to consider which techniques would be subject to its analysis, which is no doubt challenging.[335] Additionally, there are legitimate concerns that arise with having multiple theories of the Fourth Amendment—each applicable in different circumstances.[336] Nonetheless, given the "emerging technologies"[337] of government surveillance, crafting one theory to cover all methods of surveillance may hinder a court's ability to properly analyze one particular method that would more appropriately be considered under a different approach.[338]

The second, and more difficult, issue to resolve under the mosaic theory is the standard that would govern its application. Courts will have to develop a standard for determining at what point the government has gathered a

330. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring) (noting that GPS tracking reveals a wealth of information about an individual, is inexpensive, and can be used for years).

331. *Id.* at 955.

332. *Id.* at 956 ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. 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.").

333. United States v. Graham, 796 F.3d 332, 341 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

334. Selva et al., *supra* note 264, at 255 (quoting United States v. Maynard, 615 F.3d 544, 561 (D.C. Cir. 2010), *aff'd in part sub. nom. Jones*, 132 S. Ct. 945).

335. *See* Kerr, *supra* note 265, at 329.

336. *See* Curtis et al., *supra* note 63, at 89–91 (describing the issues that can develop with having different theories of Fourth Amendment law).

337. Selva et al., *supra* note 264, at 236.

338. *See* Rice, *supra* note 73, at 24 (noting that the law associated with government surveillance "may need to adapt" with advances in the technology enabling that surveillance).

sufficient amount of information such that the target's Fourth Amendment rights have been implicated.[339] In other words, the standard will determine at what point the government has conducted a "search" within the meaning of the Fourth Amendment. Assuming that warrantless CSLI monitoring is subject to a mosaic analysis, the question here, then, is what that analysis entails.

Kerr explains that Justices Alito and Sotomayor offer different standards, each reflective of their respective concerns with government surveillance.[340] He adds that courts "will have to choose"[341] one to adopt and suggests that doing so is "particularly difficult."[342]

In the context of CSLI, however, the standard should reflect the ideas of both Justices Alito and Sotomayor, as well as the underlying concerns with CSLI monitoring. More specifically, courts should adopt a "totality-of-the-circumstances" approach and analyze a nonexhaustive list of "factors" reflective of these concerns. Thus, whether all of the CSLI records obtained by police in a given case creates a "mosaic," or constitutes a "search," would depend on (1) the amount of time covered by the CSLI records,[343] (2) the amount of information that the CSLI records contained and whether it enabled the government to learn details about the target's personal life,[344] (3) the cost to the government in procuring the CSLI records and the ease with which it was able to obtain them from the service provider,[345] and (4) whether people would expect law enforcement to be able to gather the particular collection of CSLI at issue.[346]

Admittedly, this approach is not conducive to a neat and articulable standard such as the *Katz* two-prong test. However, using the totality of law enforcement behavior and outside circumstances to determine the legality of police conduct would not be a "novel" endeavor and is in fact "commonplace" within Fourth Amendment law.[347] Moreover, because the mosaic theory considers government conduct "as a collective whole,"[348] the standard for analyzing such conduct should appropriately permit consideration of all the surrounding circumstances. Additionally, because the list of factors is nonexhaustive, courts are free to add to the analysis if

339. *See* Kerr, *supra* note 265, at 329.

340. *See id.* at 330–32 (explaining the differences between the possible standards offered by the concurring opinions).

341. *Id.* at 329.

342. *Id.* at 330.

343. *See supra* notes 271–73 and accompanying text (explaining Justice Alito's emphasis on time).

344. *See supra* notes 275–77 and accompanying text (explaining Justice Sotomayor's concern with the revealing nature of location data).

345. *See supra* note 276 and accompanying text (explaining Justice Sotomayor's concern over the ease with which the government may learn about an individual's life through location data).

346. *See supra* notes 271, 276 and accompanying text (explaining Justices Alito's and Sotomayor's concern with public expectations).

347. Henderson, *supra* note 4, at 823–24 (listing areas of Fourth Amendment law where the totality-of-the-circumstances approach is used to determine whether a search or seizure has occurred, including investigatory stops and custodial interrogations).

348. Kerr, *supra* note 265, at 320.

CSLI tracking presents new concerns not addressed here. Lastly, the final factor concerning the public's expectation of CSLI monitoring specifically serves to balance the interests of cell phone users and law enforcement officials, as it can adjust according to the government's use, misuse, or disuse of CSLI monitoring.

Ultimately, however, the proposed standard does not resolve all of the issues with the mosaic theory. Nonetheless, the theory is better suited to address the concerns with CSLI monitoring than the trespass-based approach or *Katz* test. The standard and factors proposed account for these concerns and can serve as an initial consideration of how warrantless CSLI monitoring may be translated into a "search" restricted by the Fourth Amendment. Lastly, at the very least, this Note hopes that by subjecting CSLI tracking to a mosaic analysis and offering a standard under which that analysis can take place, a more complete framework for implementing the theory in CSLI-related cases can be developed.

CONCLUSION

Given that five circuit courts have almost uniformly dismissed the *Katz* test as a viable option to protect CSLI, scholars and judges should give serious consideration to new analyses with the potential to address governmental surveillance. Moreover, as technology continues to improve, it is likely that new methods of surveillance will face the same result under a *Katz* analysis because individuals in today's world disclose their location and other information to third parties in everyday activities.

In the context of CSLI, the mosaic theory provides one such alternative. This approach should be adopted as the analysis under which courts determine the legality of warrantless CSLI monitoring by law enforcement. The theory best reflects the concerns that mobile phone customers have with CSLI tracking and can serve as a viable option to protect this information.

Nevertheless, the issues that arise in administering this theory are challenging. This Note resolves some of them by proposing an open standard that courts may use to analyze CSLI under the mosaic approach. More importantly, though, this Note's efforts should serve as an invitation to other advocates of the theory to critique this standard and likewise attempt to resolve the approach's other issues. After all, as Professor Kerr rightly instructs, "proponents of the [mosaic] theory should answer" the very questions it raises.[349]

Moreover, failure to a find an alternative to the *Katz* test likely leaves CSLI without Fourth Amendment protection. Perhaps more poignantly, though, it leaves an individual's basic "right to be let alone" vulnerable to overreaching surveillance through a device people carry every second of every day.[350]

349. *Id.* at 347.
350. Katz v. United States, 389 U.S. 347, 350 (1967).