UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 96 | Number 4 Article 7

5-1-2018

All Things in Aggregation: Reassessing the Fourth Amendment's Third-Party Doctrine and the Fourth Circuit's Approach to Cell Site Location Information in *United States v. Graham*

James G. McLeod

ALL THINGS IN AGGREGATION: REASSESSING THE FOURTH AMENDMENT'S THIRD-PARTY DOCTRINE AND THE FOURTH CIRCUIT'S APPROACH TO CELL SITE LOCATION INFORMATION IN *UNITED STATES V. GRAHAM*[*]

INTRODUCTION

When technology and the law clash with one another, which wins? The measured, deliberate pace of the legal field and the often breathtakingly rapid evolution of the technological world stand in stark contrast with one another and have produced a multitude of fascinating conflicts and debates with few clear and easy answers. Applying long-standing doctrines from the age before computers to the modern world of smartphones is sometimes seamless but, in many cases, raises significant questions around the continued applicability of these doctrines. Finding answers to these questions is thus a vital task.

This struggle between rights and technology lies at the heart of *United States v. Graham*,[1] a recent Fourth Circuit case that deliberated the nature and extent of the Fourth Amendment's protection of cell site location information ("CSLI").[2] CSLI indicates the cell tower closest to a cell phone user when that user makes or receives calls and sends or receives texts, essentially creating a piece of information that details the time and place that a person makes a call or sends a text.[3] In *Graham*, CSLI collected from cell phone providers without a warrant was used to determine and track the

1. 824 F.3d 421 (4th Cir. 2016) (en banc).

2. *Id.* at 424.

3. *See* Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, THE ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/ [https://perma.cc/FC8P-ZSCE]. Historical CSLI, which is the type of data at issue in *Graham*, is created when law enforcement requests CSLI that has been generated by a particular phone. *Id.* In 2015, AT&T handled more than 58,000 requests for this historical CSLI. *Id.*

defendants' locations during a string of robberies.[4] The *Graham* court followed other recent circuit court decisions[5] by holding that law enforcement did not need to acquire a warrant for this information under the third-party doctrine,[6] a principle stating that the Fourth Amendment does not protect information individuals "voluntarily turn[] over to third parties."[7]

The *Graham* court's decision raised important questions about the conflict between privacy and a number of Fourth Amendment doctrines, including the third-party doctrine, in today's technology-driven world. Significantly, during its examination of these conflicts, the *Graham* court dismissed an argument by the defendants regarding the dangers of the aggregation of CSLI data to determine a defendant's location and track that defendant's detailed movements over a lengthy period of time.[8] To defendants, this tracking enabled by the aggregation of CSLI was the functional equivalent of long-term GPS tracking without a warrant, which is barred by the Fourth Amendment.[9] This aggregation could also raise serious privacy concerns.[10] In addition to dismissing this argument, the court further stated that the defendants improperly attempted to distinguish constitutionally protected "content" of communications (i.e., private data such as the contents of letters or the conversation of a phone call)[11] from unprotected "non-content" (i.e., the addressing information from letters or packages),[12] meaning that the court

4. *Id.*

5. *See* United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) (holding that several months of CSLI data gathered from defendants' wireless carriers was not protected because it was not content and the gathering from a third party "can only diminish the defendants' expectation of privacy in the information those records contain"), *cert. granted*, 137 S. Ct. 2211 (2017). *Carpenter*, which dealt with the gathering of CSLI information after several armed robberies throughout the Detroit area, *see id.* at 884–85, has, at the time of this writing, been granted certiorari by the Supreme Court. *See also, e.g.*, United States v. Davis, 785 F.3d 498, 517–18 (11th Cir. 2015) (finding that the defendant had "no reasonable expectation of privacy in business records made, kept, and owned by" a cell service provider); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 610–12, 615 (5th Cir. 2013) (deciding that the voluntarily-given CSLI is not protected since "it is established that, when a person communicates information to a third party *even on the understanding that the communication is confidential*, he cannot object if the third party conveys that information").

6. *Graham*, 824 F.3d at 437–38.

7. Smith v. Maryland, 442 U.S. 735, 744 (1979).

8. *Graham*, 824 F.3d at 433–34.

9. *See* United States v. Jones, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring).

10. *See id.* at 415–16.

11. *Graham*, 824 F.3d at 433.

12. *Graham*, 824 F.3d at 433.

essentially stripped all non-content third-party data—no matter how sensitive or revealing in the aggregate—of constitutional protections.[13] The lack of a boundary in this area is troublesome because a properly considered limit could resolve some of the significant fears and criticisms surrounding the third-party doctrine,[14] especially in light of the ever-evolving technologies of the modern age. Without such a limit, the government could theoretically, without the probable cause required for a warrant, obtain data from multitudes of third-party actors who collect various pieces of information about citizens in order to build an intimate, detailed picture of one's health, travels, finances, sleep schedules, contacts, internet history, purchases, and more. At this point, would the government even need a warrant?

These troubles may have been on the Supreme Court Justices' minds when they granted certiorari in the Sixth Circuit case *United States v. Carpenter*,[15] a CSLI case with many of the same concerns as *Graham*.[16] Regardless of how the Court holds, crafting a doctrine that attempts to grapple with the evolution of technology will be a difficult task. In response to the *Graham* decision and the debates surrounding the third-party doctrine and the Fourth Amendment, this Recent Development analyzes the Fourth Circuit's holding regarding the aggregation of CSLI data and discusses the potential consequences, as well as the potential remedies to these consequences.

This Recent Development's analysis proceeds in four parts. Part I provides the background of the *Graham* decision. Part II examines

13. *See id.* at 433–36 ("If individuals lack *any* legitimate expectation of privacy in information they share with a third party, then sharing *more* non-private information with that third party cannot change the calculus.").

14. *See Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 570–73 (2009) ("If third-party services play a growing role in government surveillance, the concern runs, then the Fourth Amendment will regulate a smaller and smaller portion of that surveillance; the government will be able to collect and assemble 'digital dossier' without Fourth Amendment scrutiny. To ensure sufficient constitutional protection online, many argue, the third-party cases should be overruled or sharply limited to their facts.").

15. 137 S. Ct. 2211 (2017).

16. *Compare Graham*, 824 F.3d at 425 (holding that the CSLI data gathered by police was properly gathered without a warrant because the "Court has long held that an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to [a] third part[y]'" (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979))), *with* United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) (discussing the acquisition of CSLI information by the police in a robbery case, as well as defendant's arguments that this acquisition violated the Fourth Amendment because the police did not acquire a search warrant), *cert. granted*, 137 S. Ct. 2211 (2017).

the third-party doctrine and how the Fourth and other circuits' decisions in cases regarding CSLI fit within this doctrine. Part III explores some of the potential ramifications of the *Graham* decision. Part IV proposes a different approach to the aggregation of non-content under the third-party doctrine based upon an individual's reasonable assumptions regarding how data will be used.

I. THE BACKGROUND OF *UNITED STATES V. GRAHAM*

On January 17, 2011, Aaron Graham robbed a Dollar Tree near Baltimore, Maryland at gunpoint.[17] This robbery was the first in a string of six armed robberies carried out over several weeks by Graham and a number of others throughout the Baltimore area that ended only when Graham and Eric Jordan (a fellow defendant) were apprehended after a police chase.[18] During the post-arrest investigation, the police were able to connect the defendants to the crime scenes through photographic evidence, eyewitness accounts that matched clothing worn by robbers at the crime scene with clothing found in a defendant's home and on their persons, and descriptions of the defendants' vehicle.[19] After carrying out these searches in the defendants' residences—searches conducted pursuant to search warrants—the government obtained two non-warrant court orders for "disclosure of CSLI for calls and text messages" for 221 days from both defendants' phones.[20] The defendants protested this action, arguing that the government violated the Fourth Amendment "in seeking and inspecting the CSLI at issue here without a warrant based on probable cause."[21] The Fourth Circuit, upon its initial consideration, agreed with the defendants' assertion that this gathering of CSLI was an unreasonable search, but it upheld the conviction because of the government's good faith reliance on the controlling statute, the Stored Communications Act ("SCA").[22]

17. United States v. Graham, 796 F.3d 332, 339 (4th Cir. 2015), *aff'd on other grounds*, 824 F.3d 421 (4th Cir. 2016) (en banc).

18. *Id.* at 339–40.

19. *Id.* at 340–41, 374.

20. *Id.* at 340–41.

21. *Id.* at 344.

22. *Id.* at 343. Evidence gathered in violation of the Fourth Amendment is not automatically prohibited in court. Instead, this evidence is subject to the "exclusionary rule," which bars evidence only when "the benefits of deterrence [of future violations] outweigh the costs of suppression." *Id.* at 361. This test depends on the culpability of the government's conduct, which was not sufficient to bar the evidence here due to the

The SCA, which provides a mechanism for the government to procure records or information pertaining to electronic communications,[23] allowed the government to retrieve 221 days of CSLI information for both defendants without a warrant.[24] The statute also permits a governmental entity to collect non-content information from an electronic communication service provider pursuant to a court order, which requires only "specific and articulable facts showing that there are reasonable grounds to believe" that the communications are relevant and material to an ongoing criminal investigation.[25] The SCA thus only requires that there be reasonable facts that show that communications like CSLI may be relevant to an investigation and does not require any showing that a prudent person would believe that any evidence would be found at the place of the search.[26]

Search warrants, however, require a higher standard—probable cause[27]—which exists when "there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute fruits, instrumentalities, or evidence of crime and will be present at the time and place of the search."[28] The elevated evidentiary standard for probable cause is required whenever a police action constitutes a "search" under the Fourth Amendment, which occurs when "an expectation of privacy that society is prepared to consider reasonable is infringed."[29] Such a showing is a more difficult task than merely drawing a connection of "relevancy" by reasonable facts to an investigation, which is all that the SCA requires. Thus, the government faces a lower bar to procure data like CSLI than it does to acquire evidence with a search warrant.

After analyzing the government's CSLI gathering under the SCA during its first consideration of *Graham*, a three-judge panel at the United States Court of Appeals for the Fourth Circuit found the

apparent constitutionality of the SCA's application to CSLI prior to the Fourth Circuit's ruling. *Id.* at 361–63.

23. *See* 18 U.S.C. § 2703(c)–(d) (2012).

24. *Graham*, 796 F.3d at 338, 341.

25. § 2703(c)–(d).

26. *See id.*

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

28. Doe v. Broderick, 225 F.3d 440, 451 (4th Cir. 2000) (quoting United States v. Suarez, 906 F.2d 977, 984 (4th Cir. 1990)).

29. Maryland v. Macon, 472 U.S. 463, 469 (1985) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

access to CSLI information constituted a search under the Fourth Amendment.[30] Since searches generate more stringent Fourth Amendment protections, the panel reasoned, the SCA's lower standard for collecting CSLI was constitutionally insufficient—instead, a warrant was needed.[31] The panel's holding was guided by its concerns regarding the government's ability to use CSLI to trace the movements of an individual for a long period of time.[32] In addition, such aggregation and long-term tracking could lead to the discovery of individuals' private lives and personal habits, and the court felt that cell phone users have a reasonable expectation that such private matters will remain private and not be inspected by the government without a warrant.[33] Finally, the panel believed that the CSLI information at issue was not voluntarily conveyed at all—the "mere fact that the information [wound] up in the third party's records" was not sufficient for voluntary conveyance by an individual.[34] This decision, however, did not go unchallenged.

After the Fourth Circuit's initial ruling that the gathering of CSLI constituted a search that required a warrant, the government requested a rehearing en banc by the Fourth Circuit to fully consider the Fourth Amendment question, which the court granted.[35] The Fourth Circuit subsequently upheld the conviction, but it established that the collection of the data did not, in fact, violate the Fourth Amendment, thus overturning the initial ruling.[36] The court recognized that a Fourth Amendment search occurs when the "government violates a subjective expectation of privacy that society recognizes as reasonable," but this protection ends when information is "voluntarily turned over to a third party."[37] It determined that the CSLI was, in fact, "voluntarily" conveyed to a third party because of defendants' understanding that cell phone calls necessarily send out location information[38] and that the defendants had "assumed the risk"

30. United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015), *aff'd on other grounds*, 824 F.3d 421 (4th Cir. 2016) (en banc).

31. *Id.* ("Appellants argue that the government violated the Fourth Amendment in seeking and inspecting the CSLI at issue here without a warrant based on probable cause. We agree.").

32. *Id.* at 345.

33. *Id.*

34. *Id.* at 353–55.

35. United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (en banc).

36. *Id.*

37. *Id.* at 425, 427 (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

38. *Id.* at 430.

of the information being provided to the authorities.[39] The court also addressed the difference between content and non-content in electronic communications but held that the CSLI was not communications content, which has constitutional protections.[40] It stated that even though the CSLI could be "aggregated" to determine the location of defendants over a long period of time, precedential cases allowed the same sort of effect to pass constitutional muster, and that the defendants attempted to "blur" the distinctions between non-content and content with their arguments.[41] With this holding, the court essentially removed CSLI information from the protections of the Fourth Amendment, meaning the government need only meet the lower SCA evidentiary standard to gather such data in future cases.

II. THE THIRD-PARTY DOCTRINE, THE CONTENT/NON-CONTENT DISTINCTION, AND THE *GRAHAM* DECISION

Understanding why the Fourth Circuit dismissed Graham's arguments requires a brief look at the background and development of the third-party doctrine and the content/non-content distinction. In addition to this doctrinal overview, this Part concludes with an examination of the unclear future of the third-party doctrine.

A. The Third-Party Doctrine of the Fourth Amendment

In 1967, the Supreme Court moved away from a strict textual interpretation of the protections provided by the Fourth Amendment, which focused on whether or not a "trespass" had occurred to a more subjective, privacy-based test in *Katz v. United States*.[42] This new

39. *Id.* at 427.

40. *Id.* at 433–34. The contents of various mediums of communications—including the contents of letters and packages, telephone calls, and emails—are protected under the Fourth Amendment, but non-content information, i.e., routing or address information, is not. *Id*. at 433. The fact that contents are "sealed" in order to be "fully guarded from examination and inspection . . . as if they were retained [by the communicator] in their own domiciles" gives these contents Fourth Amendment protection. *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding that the contents of letters are protected by the Fourth Amendment).

41. *Graham*, 824 F.3d at 433–34.

42. 389 U.S. 347 (1967). Prior to *Katz*, the Supreme Court had followed a narrow "trespass" doctrine that put only physical trespasses and seizures of material objects within the purview of the Fourth Amendment. *See id.* at 352–53; *see also* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 6 (2014). Prior to *Katz*, the Fourth Amendment was only understood to protect "persons, houses, papers, and effects." *Id.*

subjective test was articulated in a concurrence by Justice Harlan and asked first whether a person had "exhibited an actual (subjective) expectation of privacy and, second, [whether] the expectation [was] one that society is prepared to recognize as 'reasonable.'"[43] However, the Court also held that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[44]

Applying this doctrine in a subsequent case, the Court held that a warrant was not required to access bank checks and deposit slips, as they were "not confidential communications" but were instead "negotiable instruments to be used in commercial transactions."[45] While these banking records may at first glance seem quite confidential to consumers, the fact that these checks and slips still consisted of information voluntarily conveyed to a third party rendered them unprotected by the Fourth Amendment.[46] Going even further, the Court determined in a later case, *Smith v. Maryland*,[47] that the use of a pen register—a device designed to register, record, and disclose the numbers dialed on a phone[48]—did not constitute a search and was not a violation of the Fourth Amendment.[49] The court reasoned that the defendant had "no actual expectation of privacy in the phone numbers he dialed" and that he had voluntarily conveyed the numbers to the phone company, which lowered the expectation he could have in the privacy of the numbers.[50]

Analogizing the CSLI at issue to bank records and phone numbers, the *Graham* court found this data to be unprotected by the Fourth Amendment because of the third-party doctrine, which meant that no warrant was needed.[51] Like the bank records conveyed in *Smith*, the CSLI was voluntarily conveyed by the defendants, who broadcast their locations through their texts and calls and thus took the risk of this information's recordation by a third party. The lack of

43. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also Graham*, 824 F.3d at 425 (applying the *Katz* expectation of privacy test).

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

45. *See* United States v. Miller, 425 U.S. 435, 442 (1976) ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

46. *Id.* at 442–43.

47. 442 U.S. 735 (1979).

48. *Id.* at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

49. *See id.* at 744–46.

50. *See id.* (using *Miller* as analysis to determine that the defendant voluntarily conveyed numerical information to the telephone company through his dialing).

51. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc).

Fourth Amendment protection for voluntarily conveyed information, established in *Miller* and *Smith*, underpins the third-party doctrine at issue in *Graham* and explains the court's refusal to apply Fourth Amendment protections to the data.

Another way to understand the *Graham* court's refusal to protect the CSLI is by exploring the lack of protections given to "business records" under the third-party doctrine. The third-party doctrine roughly includes two lines of cases.[52] The first line (which is not at issue here) pertains to information given to so-called "secret agents," who are undercover police agents or informants.[53] The second line, and the one through which cases like *Graham* have been decided, fall within the "business record" line of cases, which find that information voluntarily conveyed to another party in the ordinary course of business have no Fourth Amendment protections.[54] Both the bank records in *Miller* and the data produced by the pen register in *Smith* were found by the respective courts to be business records.[55] This analysis has been extended to cases confronting CSLI data gathering[56] and can apply to any number of other entities that may reasonably retain records about customers or subscribers.[57] Under this doctrine, people cannot have a reasonable expectation of privacy in information disclosed to a third party that are classified as business records.[58]

An important distinction must be made between these business records and confidential communications to other parties, however. When a third party is an "intermediary," or service that handles a communication, the communication is not deemed to have been given

52. *See* Kerr, *supra* note 14, at 566.

53. *See id.* at 567–68. This line of cases essentially holds that statements made to undercover officers or informants are not protected by the Fourth Amendment and do not require any sort of warrant, as "one contemplating illegal activities must realize and risk that his companions may be reporting to police." *Id.* at 568.

54. *See id.* at 569.

55. *See id.* at 569–70.

56. *See* United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) ("This case involves business records obtained from a third party, which can only diminish the defendants' expectation of privacy in the information those records contain."), *cert. granted*, 137 S. Ct. 2211 (2017).

57. *See* United States v. Graham, 824 F.3d 421, 435 (4th Cir. 2016) (en banc) ("Indeed, we expect that our banks, doctors, credit card companies, and countless other third parties will record and keep information about our relationships with them, and will do so for the entirety of those relationships—be it several weeks or many years . . . . This is true even when, in the aggregate, these records reveal sensitive information similar to what could be revealed by direct surveillance.").

58. Kerr, *supra* note 14, at 563.

over to a third party, and the government must have a warrant to access the contents.[59] "Simple business records," however, and information given to an intended recipient to be used "in the ordinary course of business" do not have the same reasonable expectation of privacy and may thus be obtained by the government without probable cause and a warrant.[60] This distinction is why business records like CSLI may be gathered from a business without a warrant, while the contents of letters, phone calls, and emails may not, even though these communications travel through the business's networks or servers.

All told, these lines of reasoning and doctrines explain why, when confronted with an issue regarding CSLI and Fourth Amendment protections, the *Graham* court found that the acquisition of CSLI from a cell-service provider did not require a warrant to be gathered.

B. The Content/Non-Content Distinction

A separate doctrine—the content/non-content doctrine—also plays a role in Fourth Amendment protections, as seen in *Graham*. The CSLI data in *Graham* was routing information that was deemed mere non-content data and therefore does not receive the same Fourth Amendment protections as the contents of other communications.[61] This content/non-content doctrine protects the contents of communications from government surveillance without a warrant and finds its roots in case law regarding letters.[62] The sealed nature of letters and similar packages makes the contents "'as fully guarded from examination and inspection' as it would be if the party mailing the letter had retained it in his or her own home."[63] The sealed and confidential nature of such communications grants the public a "legitimate expectation of privacy" in such communications, even though the entrusting of the letter to an intermediary (i.e., the post office) means that the letter or communication could be easily accessed.[64] This content doctrine has been expanded to digital

59. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the contents of emails have a reasonable expectation of privacy).

60. *See id.*

61. *See Graham*, 824 F.3d at 433–34

62. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009).

63. *Id.* (citing *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

64. *See Warshak*, 631 F.3d at 285–86 (holding that the contents of emails are protected by the Fourth Amendment).

communications like emails,[65] as well as non-text based communications like phone calls.[66] Non-content, however, may be accessed by the government without a warrant.[67] Non-content includes phone numbers dialed by a party, the exteriors of packages and letters, and routing information.[68] Non-content is not protected because there is no "actual expectation of privacy" for this information because of the understanding that it is provided or visible to a third party.[69]

The defendants in *Graham* attempted to argue that the CSLI should have been treated as content instead of non-content by the court, as CSLI "record[s] a person's movements over a prolonged period" and that this greater detail raises serious privacy concerns, essentially transforming non-content into content.[70] The negative implications of these privacy concerns are summed up by Justice Sotomayor in her *United States v. Jones*[71] concurrence when she questioned whether movements should be aggregated to the point that the government could determine intimate details of the lives of individuals, including political and religious beliefs, sexual habits, and much more.[72] This aggregation argument made by the *Graham* defendants closely mirrors a theory of Fourth Amendment analysis known as the "Mosaic Theory."[73] This theory focuses on law enforcement actions in their entirety, rather than looking at these actions individually,[74] and has been used as a rationale for Fourth Amendment searches by at least one circuit court.[75] However, the court in *Graham* found that even though *all* routing information records "potentially sensitive activity when aggregated" and that, even though CSLI is "not identical to . . . other . . . routing

65. *See id.*

66. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013).

67. *See* United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016) (en banc).

68. *Id.*

69. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."). For a further exploration of the content/non-content distinction in other areas of technological change, see generally Tokson, *supra* note 62.

70. *Graham*, 824 F.3d at 433–34 (alteration in original).

71. 565 U.S. 400 (2012).

72. *See id.* at 416 (Sotomayor, J., concurring).

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

74. *Id.*

75. *See* United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 565 U.S. 400 (2012).

information," it "blinks at reality" to argue that CSLI constitutes a "communication of content."[76] Because the CSLI was made up of routing information and contained no content, the court determined the information to be non-content.[77] However, although it is unlikely that the content/non-content distinction will be eliminated, recent legal events have cast doubt on the future of the Fourth Amendment doctrines used by the *Graham* court, as well as the analyses and applications of these doctrines.

C. The Muddled Future of the Third-Party Doctrine

The future of the third-party doctrine has recently been called into question, both in regard to its application to the gathering of CSLI and to its future as a whole, by the recent decision of *United States v. Jones*[78] and the recent grant of certiorari by the Supreme Court in *Carpenter v. United States*, a United States Court of Appeals for the Sixth Circuit case that also grappled with the Fourth Amendment's application to CSLI.[79] *Jones* demonstrated that a number of justices may be willing to reassess the third-party doctrine if given the chance.[80] Justice Sotomayor stated concerns about whether people "reasonably expect" their movements to be recorded to such a degree that the government could ascertain intimate details about their lives, including "their political and religious beliefs, sexual habits, and so on."[81] Justice Alito—speaking for three other Justices—argued that long-term GPS government tracking constituted a search and could thus not be gathered without a warrant.[82]

The Supreme Court's grant of certiorari in *Carpenter*, a case remarkably similar to *Graham*, indicates that some sort of significant change for the third-party doctrine may be on the horizon, especially in light of the views expressed in *Jones*. The *Carpenter* court found a number of defendants guilty of committing a string of armed

76. United States v. Graham, 824 F.3d 421, 434 (4th Cir. 2016) (en banc).

77. *Id.*

78. 565 U.S. 400 (2012). The Supreme Court unanimously held a GPS tracker on a vehicle used to monitor a movement was "a search . . . within the meaning of the Fourth Amendment." *Id.* at 402.

79. 819 F.3d 880, 884 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

80. *See* THOMPSON II, *supra* note 42, at 21–22.

81. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

82. *See id.* at 430. (Alito, J., concurring) ("We need not identify . . . the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

robberies throughout the Detroit area and featured the same sort of warrantless gathering of CSLI information pursuant to the SCA to pinpoint the defendants' location near the scenes of the crimes.[83] The Sixth Circuit upheld the convictions on appeal and found that the collection of CSLI was a collection of business records and therefore not a search under the Fourth Amendment.[84] The Supreme Court granted this case certiorari and recently heard oral arguments.[85]

Justice Sotomayor, in her *Jones* concurrence, has already expressed deep reservations about the third-party doctrine and its applicability in the digital age,[86] and Justices Ginsburg, Kagan, and Breyer joined Justice Alito's opinion that expressed his own concerns about long-term government surveillance in *Jones*.[87] The CSLI gathered in *Carpenter* was not gathered through any sort of government surveillance, but the practical effect of the information gathered still allowed law enforcement to create a map that showed the defendants' movements over nearly a six-month period.[88] With their concerns around steady, lengthy location surveillance,[89] this group of Justices may attempt to find a way to prevent CSLI aggregation that essentially mirrors the GPS surveillance seen in *Jones*. One other distinction the *Carpenter* circuit court drew between the GPS in *Jones* and the CSLI before them was the relative lack of accuracy and precision of CSLI versus GPS surveillance, with GPS being accurate to within fifty feet while CSLI tracking could only pinpoint a generalized area.[90] To the court, this distinction was fatal to the defendants' arguments, and the court declined to speculate about any future technologies.[91] However, some of the Justices in *Carpenter*'s oral arguments did speculate about future technologies and the degree of precision that CSLI could achieve, with Justice Kagan recognizing that technology had already progressed since the

83. *Carpenter*, 819 F.3d at 884–85.

84. *Id.* at 890.

85. Transcript of Oral Argument, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).

86. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

87. *See id.* at 430 (Alito, J., concurring).

88. *Carpenter*, 819 F.3d at 884–85.

89. *See Jones*, 565 U.S. at 417 ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

90. *See Carpenter*, 819 F.3d at 889.

91. *See id.*

initial events of *Carpenter* to potentially allow tracking in a space half the size of the Supreme Court's courtroom.[92]

Other Justices, including newly appointed Justice Gorsuch, attempted to explore more exotic alternatives during *Carpenter*'s oral arguments,[93] and many of the Justices further pressed the counsel for the government about their concerns with long-term tracking.[94] However, the Justices pressed the counsel for the petitioner just as hard with their concerns about overturning precedent[95] and on the difficulties of creating a line or distinction to find government tracking unconstitutional without a warrant,[96] as well as the distinction between location information and the business records in *Miller*.[97] All told, the Justices, respondents, and petitioners grappled with many of the same issues and faced many of the same decisions that the *Graham* court faced. The consequences of some of these decisions—especially if the Supreme Court's decision mirrors that of *Graham*—as well as some potential solutions are the focus of the remainder of this Recent Development.

III. CONSEQUENCES AND CRITICISMS OF *GRAHAM*

The Fourth Circuit claimed that the intention of the defendants in *Graham*, when they argued that the aggregation of CSLI was content, was to "blur this clear distinction" between content and non-content, and asserted that "[c]onstitutional distinctions are made of sturdier stuff" than that which was put forth by the defendants in their arguments.[98] However, the current constitutional distinction is gravely lacking. As technology progresses, the line between non-content and content is likely to grow ever more blurred. This content/non-content distinction was created to guarantee the right of people to be "secure in their papers . . . thus closed against inspection,

92. Transcript of Oral Argument at 72, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).

93. *See id.* at 51–52 (beginning a line of questioning in which Justice Gorsuch moved away from the reasonable expectation of privacy approach and instead attempted to explore with counsel for the respondent whether or not a defendant may hold a property right in her location information).

94. *See id.* at 48, 66, 70 (providing the concerns of Justices Sotomayor, Breyer, and Kagan respectively).

95. *See id.* at 15 (questioning, by Justice Alito, about how much precedent the petitioners want to overrule).

96. *See id.* at 7–15.

97. *See id.* at 4–6.

98. United States v. Graham, 824 F.3d 421, 434 (4th Cir. 2016) (en banc).

wherever [the papers] may be."[99] Dismissing the defendants' argument without any great consideration of the merits ignores the importance of defendants' interest in their effects and papers, be they technological data or other types of personal information in which parties have a reasonable expectation of privacy. Furthermore, this could be potentially problematic for the future of Fourth Amendment protections. A distinction that does not provide security to the contents of communications and other sensitive information ignores the very rationale behind the protections given to content in the first place.

A. The Third-Party and Content Doctrines in the Twenty-First Century

As the modern world becomes more technologically advanced and interconnected, an ever-increasing amount of potential non-content data will be produced by technological innovations that may fall under the scope of the third-party doctrine.[100] In his dissent in *Graham*, Judge Wynn addressed this concern head-on by describing several examples specific to cellular devices that could potentially lead to far more precise location information.[101] For example, tiny "microcells"—cell sites small enough to coat roofs, interior flooring, and other areas—as well as smartphone "pinging," through which smartphones are in almost continuous contact with cell towers regarding their location, could all lead to instantaneous, precise tracking of a defendant.[102] In Judge Wynn's view, this sort of precise tracking would be allowed under the court's ruling.[103] He further raised a concern about the scope, detail, and length of the tracking enabled by the aggregation of CSLI.[104]

99. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

100. *See generally If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924 (2017) (discussing the lack of Fourth Amendment protection of personal digital records shared with third parties via home automation).

101. *Graham*, 824 F.3d at 448 (Wynn, J., dissenting).

102. *Id.*

103. *Id.* at 448–49. Judge Wynn was concerned that the majority did "not decide . . . that the CSLI employed here was too imprecise or too discontinuous to infringe Defendant's privacy," which he believed would allow incredibly precise and continued tracking under new technologies under the court's ruling. *Id.*

104. *See id.* at 447. This long-term tracking also brings to mind the GPS tracking in *Jones* which concerned Justice Alito, who claimed that four weeks of GPS tracking of a vehicle was a search. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring). *But see Graham*, 824 F.3d at 435 ("But *Jones* involved *government*

Other circuit court judges have expressed similar concerns. For example, Judge Martin's dissent in *United States v. Davis*,[105] a case from the Eleventh Circuit, supports Judge Wynn's argument and described the extensive amount of information that Google (as well as Facebook, Amazon, and other sites) gathers. This information includes websites visited, personal and financial information, the specific type of electronic devices used by individuals (i.e., whether a person was using their smartphone or laptop), and one's actual location. The dissent highlighted the fact that, under the third-party doctrine, all of this data could be gathered by the government without a warrant.[106] But that is not the end of the problem.

The biggest concerns regarding non-content data do not arise from what information law enforcement can access now, but rather what they will be able to access in the very near future. "[C]onnected TVs, refrigerators, appliances, [and] home automation systems" already exist.[107] Smart mattresses that monitor sleep patterns and share this data with your phone have been developed, as have smart cars that will be connected to cellular companies' networks.[108] Perhaps most intimate, however, is the range of health trackers, from the already-used Fitbit fitness tracker to devices like personal EKG monitors, to glucose monitoring systems that can send detailed ten-day analyses of one's health patterns to doctors.[109] While the precise readings and contents of any messages created by these devices would be protected, other information shared with third parties from these devices could, under the *Graham* court's test, be discovered by police without a warrant if they were found to be "voluntarily conveyed."[110] All of this could be aggregated to paint an intimately detailed portrait of a person's life. In other words, while the contents of any messages created by these devices may be protected, the aggregation of any non-content data and messages over time could essentially render the protections provided to the contents of communications moot. The

surveillance of an individual, not an individual's voluntary disclosure of information to a third party.").

105. 785 F.3d 498, 533–45 (11th Cir. 2015) (Martin, J., dissenting).

106. *See id.* at 534; *see also In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 623 (4th Cir. 2013) (Dennis, J., dissenting) (providing further examples of concerns).

107. Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (Jan. 13, 2014), http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/ [https://perma.cc/8YSC-HMQZ].

108. *See id.*

109. *See id.*

110. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc).

access to the contents of messages requires probable cause so as to prevent the sealed and guarded contents of those letters from being accessed by the government;[111] allowing an aggregation of non-content data to the point that contents can essentially be read, guessed, or easily determined circumvents these protections. To so easily overcome these protections goes against the spirit and purpose of the Fourth Amendment.

For instance, consider a theoretical health device worn on the wrist that is capable of reading a number of vital health indicators.[112] The benefit of this device is that it automatically sends an alert to any number and type of a large list of doctors regarding changes in the wearer's vital signs, allowing the doctors to immediately determine if the wearer needs medical treatment, what type of medical treatment, and the severity of the situation. Imagine that this device has quickly become ubiquitous in modern society due to its ability to recognize strokes, heart attacks, the onset of seizures for epileptics, and changes in blood sugar in diabetics, as well as its general day-to-day usage by the population as a fitness and health tracker. The company that produces these devices also produces specialty versions of the device, such as one that tracks important health statistics in pregnant mothers and sends daily reports to the mother's OB/GYN to monitor the pregnancy's progress and the health of the fetus. The company does not have access to the health readings themselves but does choose to keep logs of which wearer sends messages to which doctors in order to run diagnostics on its network and keep track of the effectiveness of the system. The company pledges to its customers that no contents of any alert or message to any healthcare provider can be accessed, stored, or retained by the company in any way.[113]

111. *See supra* Section II.B.

112. While the device provided in this hypothetical does not currently exist and was created by the author to illustrate the third-party doctrine and content/non-content distinctions, some of these technologies currently exist and are in use today. *See, e.g.*, Bertalan Mesko, *Top 10 Healthcare Wearables for a Healthy Lifestyle*, THE MED. FUTURIST, http://medicalfuturist.com/top-healthcare-wearables/ [https://perma.cc/CB9P-V4PX].

113. Whether or not HIPAA would cover the data tracked by such a device would largely depend upon whether or not the device's manufacturer is a "covered entity" or not. *See* Kristen Lee, *Wearable Health Technology and HIPAA: What Is and Isn't Covered*, TECHTARGET (July 2015), http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/8SVA-VQH7]. Under this rule, commercially purchased devices would usually not fall under HIPAA, while devices provided by a health care provider, doctor, or other similar entity would. *See id.* Regardless, HIPAA has separate disclosure rules that allow law enforcement to procure

However, such a device could still be used by the government to gather an intimate and exhaustive picture of one's health. The communications logs kept by the company are analogous to the location information kept by the cell phone companies in *Graham* and the phone numbers dialed in *Miller* because they are considered "addressing" and "routing" information.[114] Furthermore, the statute that allowed the police to acquire CSLI in *Graham*,[115] the SCA, could be used to acquire this information, as the SCA allows the government to access records of a customer from an electronic communication service.[116] The information gathered by the government through this method would only be the routing information between the device's wearer and her doctors and would not include the contents of the messages (in this case, the exact readings of the device), but even this routing information could provide the government with an intimate look into the life of the wearer after its aggregation. For instance, continuous communications between a wearer and an OB/GYN could make it possible to determine that one is either pregnant or considering pregnancy, while a sudden flurry of messages towards surgeons and cardiologists could signify a heart problem or an array of other significant ailments that a wearer may wish to keep private. While such clues and aggregations may not be completely accurate or as telling as the actual content of any message would be, enough data points could still reach a point where the government has little doubt about the meaning behind the communications. All of these individual data points could, in the aggregate, provide the government with an intimate look into the personal health and well-

certain personal information during investigations. *See* 45 C.F.R. § 164.512(f) (2017) (describing the requirements for disclosure of medical information to law enforcement, including personal information "in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect").

114. *See Graham*, 824 F.3d at 433 ("The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information . . . . CSLI, which identifies the equipment used to route calls and texts, undeniably belongs in the non-content category.").

115. *See id.* at 426.

116. *See* 18 U.S.C. § 2703(c) (2012) ("A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the content of communications)."). An "electronic communication service" is defined elsewhere in the statute as "any service which provides to users thereof the ability to send or receive wire or electronic communications." § 2510(15).

being of any party using these devices without any Fourth Amendment barriers.

An example like this runs into a clear counterargument that asks whether or not data of this type is even relevant to police surveillance and the Fourth Amendment. However, any such relevance would not have to be significant—law enforcement would only have to provide "specific and articulable" facts that the data is relevant to an ongoing case to pull the data from this device,[117] meaning the bar for access to the information would not be high if law enforcement were to find any reason to collect the data. In any event, this scenario still provides a framework for how such modern devices could be accessed by law enforcement without meeting the threshold of probable cause. Furthermore, the same sort of analysis could work for any variety of different devices, from pinging GPS devices installed in cars to devices that track IP addresses.[118] In the era when a folded map functioned as one's global positioning system and letters and rotary phones were the primary means of contacting others, the costs of aggregation—of gathering sufficient data to craft a mosaic of a person's life—were steep, inconvenient, and time-consuming. Now, however, modern technology makes the creation of a multi-faceted portrait far simpler.

B. Keeping the Current Doctrine Has Consequences, but so Too Does Change

Proponents of the third-party doctrine and detractors of the concerns about aggregation may claim that data of this nature still falls clearly under the third-party doctrine and, while intimate and possibly concerning, the data is still composed of non-content and thus cannot require a warrant.[119] Under the very broad lines laid

117. *See* § 2703(d) ("A court order . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

118. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that using a device that tracked the IP addresses typed and accessed by a defendant was "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*" and that the action of tracking IP addresses thus did not require a warrant).

119. *See Graham*, 824 F.3d at 433 ("CSLI is non-content information because 'cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves.'" (quoting United States v. Carpenter, 819 F.3d 880, 887–88 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017))).

down in *Graham*, they would be correct,[120] as the Fourth Circuit believes that people today "expect that . . . countless other third parties" will retain information about them that may not remain secret.[121] Proponents of the third-party doctrine have argued that it provides clarity and a test that is easy to apply and have pointed to the fact that an alternative has not been easily created as evidence of the doctrine's validity.[122] They also argue that due to the rapidly evolving pace of technology, a doctrine that attempts to draw a line after aggregation is untenable.[123]

An additional difficulty revolves around the practical application of any aggregate or mosaic theory.[124] Proposing that judges apply complex constitutional tests to determine whether or not the Fourth Amendment has been violated may only place a heavy burden onto judges, who must then try to make sense of complex constitutional doctrines and factual situations without a clear test or line.[125] Bright line tests like the third-party doctrine are easy to administer: if the information has been given to a third party, it is unprotected. This test is simple to use, predictable in result, and does not impose a heavy burden on judges to determine the constitutionality of an action. However, clarity, simplicity, and ease of application do not guarantee a doctrine's faithfulness to the Constitution. The protections provided by the Fourth Amendment should be the keystone for any doctrine, not the simplicity of application.

The current doctrine may be simple to apply, but it ignores growing practical modern realities. The Fourth Circuit and other courts have found that an individual has no actual expectation of privacy when she "voluntarily conveys" information like CSLI,[126] phone numbers,[127] or IP addresses,[128] even when she does not recognize that she is actively conveying this information to a third party.[129] According to the Fourth Circuit, this is true even when "in the aggregate, these records reveal sensitive information similar to

120. *See id.* at 432.
121. *Id.* at 435.
122. *See* Kerr, *supra* note 14, at 581.
123. *See* Kerr, *supra* note 73, at 347–48.
124. *See id.* at 346–47.
125. *See id.*
126. *See Graham*, 824 F.3d at 430.
127. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).
128. *See Graham*, 824 F.3d at 432.
129. *See id.* at 430.

what could be revealed by direct surveillance."[130] The constitutional protections that require the government to acquire a warrant to access "communications content" (such as the contents of sealed mail or emails) still exist,[131] but the fact remains that these protections become ineffective if the government can use unprotected non-content information to essentially determine what the protected communication may say. In *Graham*, for instance, the government has already shown an ability to closely track a defendant using CSLI alone.[132]

An acceptance of this concept ignores Justice Sotomayor's concerns in her *Jones* concurrence regarding the government painting a precise picture of one's life, including their "political and religious beliefs, sexual habits, and so on."[133] It also ignores Justice Alito's concern about the rapid decline of what was once one of the most significant protections of privacy from government surveillance: the technological capabilities of the government itself.[134] Months-long surveillance efforts would once have taken massive police resources and would be reserved for only the most significant crimes; now, however, the government can use CSLI and other data to essentially track a defendant for weeks without spending significant resources, greatly expanding the ability of the government to track citizens.[135] The long-held societal expectation that "law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period" in this manner was a key rationale for Justice Alito when he held that continuous government surveillance for four weeks without a warrant was unconstitutional under the *Katz* test.[136] Courts have correctly held that *Jones* only places these restrictions on long-term government surveillance and tracking,[137] but this distinction provides little solace for defendants.

Creating a detailed account of one's life from data taken from a GPS installed by police versus information taken from a phone

130. *Id.* at 435.

131. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013).

132. *See Graham*, 824 F.3d at 447 (Wynn, J., dissenting).

133. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

134. *See id.* at 429 (Alito, J., concurring) ("Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

135. *See id.*

136. *Id.* at 430–31.

137. *See Graham*, 824 F.3d. at 435 ("But *Jones* involved *government* surveillance of an individual, not an individual's voluntary disclosure of information to a third party.").

company seems like a small distinction, but according to current doctrine, it is sufficiently different for defendants to entirely surrender their *actual* expectation that their every move not be followed.[138] The fact that this small difference in action creates such a vast difference in expectations of privacy and in doctrinal results presses the boundaries of reasonableness. With a rise in information transmitted to third parties by technological devices, the government may be able to find out far more about a person than it once could have with a warrant. The *Graham* court worried about blurring the line between content and non-content and approved of a clear distinction,[139] but at some point this non-content, when aggregated, could potentially tell just as much—if not more—than content ever could, as demonstrated by the health device hypothetical given above. At that point, there may be no distinction between content and non-content at all.

Regardless of whether or not the information collected by all of these sources falls under the traditional third-party doctrine, the end effect may be an erosion of Fourth Amendment protections. As established in *Katz*, the Fourth Amendment provides protections when persons have "exhibited an actual (subjective) expectation of privacy" and when that expectation is one that "society is prepared to recognize as 'reasonable.'"[140] However, if all information given to third parties, even unknowingly, is considered to be "voluntarily conveyed," where does one's actual and reasonable expectation of privacy end and begin? The Fourth Circuit's decision in *Graham* (as well as those similar decisions in other circuits), and the aggregation of non-content that it allows, could paint such a detailed picture of a potential defendant's life that one's "persons, houses, papers, and effects"[141] could be laid bare for the government, all without a warrant. Regardless of whether or not this information is voluntarily conveyed, it would be a return to the days of unlimited government searches[142] to allow this to continue unchecked.

138. *See id.* at 433; United States v. Davis, 785 F.3d 498, 514 (11th Cir. 2015).

139. *See Graham*, 824 F.3d at 433 n.12 ("[T]he content/non-content distinction makes good doctrinal sense. The intended recipient of the content of communication is not the third party who transmits it, but the person [who is] called . . . . The routing and addressing information, by contrast, is intended for the third parties who facilitate such transmissions.").

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

141. U.S. CONST. amend. IV.

142. *See* THOMPSON II, *supra* note 42, at 3–4. Thompson laid out the history behind the passage of the Fourth Amendment, describing "indiscriminate government intrusions" by

IV. A POSSIBLE LEGAL RESPONSE MOVING FORWARD

Finding a response to these changing circumstances is contentious[143] and resists a simple test.[144] However, to ignore the problem would be an improper response. Instead, the best way forward is likely that option touched upon by Justice Sotomayor in *Jones* when she asked "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain . . . their political and religious beliefs, sexual habits, and so on."[145] People may have an expectation that seemingly insignificant individual data points, such as the numbers they call, will be recorded or monitored, but aggregating these data points to create an intricate description of one's life that essentially circumvents the content protections is surely not "reasonable." However, these aggregations are allowed under the current case law, including *Graham* and *Carpenter*. Thus, a change is needed to truly protect individuals' Fourth Amendment rights.

A. A Proposed Test: Does One Have a "Reasonable Assumption" of Privacy?

This Recent Development suggests that courts adopt a rule that allows non-content to still be acquired without a warrant but not to a point that the non-content could be aggregated into a picture which, for all intents and purposes, conveys what the contents of messages would have. Such an aggregation approach has already been attempted by the D.C. Circuit in *United States v. Maynard*,[146] the circuit court decision that eventually became the Supreme Court case *United States v. Jones*. The D.C. Circuit held that the aggregated movements of the defendant required a warrant.[147] All told, the

the British into private homes that led to "fear of unrestrained government power" and to the eventual passage of the Fourth Amendment in response. *Id.*

143. *See, e.g.*, *Graham*, 824 F.3d at 441–50 (Wynn, J., dissenting); United States v. Davis, 785 F.3d 498, 533–45 (11th Cir. 2015) (Martin, J., dissenting); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615–32 (4th Cir. 2013) (Dennis, J., dissenting).

144. See the lack of a unified test in *United States v. Jones*, 565 U.S. 400, 402–31 (2012) (establishing a traditional "trespass" test via Justice Scalia, a *Katz* reasonableness test with a concern for aggregation by Justice Sotomayor, and a traditional reasonableness test by Justice Alito).

145. *Id.* at 416 (Sotomayor, J., concurring).

146. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 565 U.S. 400 (2012).

147. *Maynard*, 615 F.3d at 556–58. The D.C. Circuit found that the most significant factor in whether a party has a reasonable expectation of privacy for information is whether that information "has been exposed to the public." *Id.* at 558. Furthermore, what

defendant had a reasonable expectation of privacy under the *Katz* test, and the "prolonged GPS monitoring reveal[ed] [such] an intimate picture of the subject's life" that the court found the monitoring to be a search.[148] This aggregation approach, subsequently dubbed the "Mosaic Theory," analyzes police actions as a collective instead of individually.[149] If the actions taken by police reach the level of a Fourth Amendment search as an entirety, a warrant is needed, even if each of the individual actions would not have independently required a warrant.[150] This approach shows how such an aggregation approach may work and serves as evidence that some courts are currently responsive to the idea.

This Recent Development's proposed test incorporates the idea of aggregation that concerned Justice Sotomayor in *Jones*[151] and the D.C. Circuit in *Maynard*,[152] and it will be called the "reasonable assumption" test. The foundation for this test finds its roots in Justice Marshall's dissent in *Smith*, in which he argued that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited purpose need not assume that this information will be released to other persons for other purposes."[153] Parties who provide their location by making a phone call should reasonably know that their information may be used to locate them at the location of the call. This fact has been well established and developed by the courts[154] and should allow this immediate-location data to still be accessible by the police under both the third-party and non-content doctrines. However, courts should recognize that customers who provide their location for a phone call have a reasonable *assumption* that their phone calls will not eventually be used and aggregated by the police to intimately track their movements over a long period of time. While

the police discovered—the month-long movements and location discussed in *Jones*—was not exposed to the public, as the "whole of one's movements over the course of a month is [neither] *actually* exposed" nor "constructively" exposed, even though each individual movement was, in fact, exposed. *Id.*

148. *Id.* at 563.

149. Kerr, *supra* note 73, at 313. For more background and general analysis into the Mosaic Theory, as well as an ultimate rejection by Professor Kerr, see generally *id.*

150. *Id*. at 336–40.

151. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

152. *See Maynard*, 615 F.3d at 556–58.

153. *Smith v. Maryland*, 442 U.S. 735, 749 (1978) (Marshall, J., dissenting).

154. *See* United States v. Graham, 824 F.3d 421, 430 (4th Cir. 2016) (en banc) (discussing both the facts at hand, as well as other cases that held that parties understand their exposing of location through phone calls).

there may be a reasonable expectation that such a thing *could* be done, they would also have a reasonable assumption that such a thing *would not* be done because of their constitutional right to be "secure in their persons, houses, papers, and effects" against unreasonable searches[155] and because of the vastly different and more intimate picture that such an aggregation paints, as compared to a single data point. Thus, the dividing line between a gathering of non-content given to third parties and an unconstitutional search or intrusion into what is essentially the "contents" of messages would be what the subjective person would reasonably assume the original information would be used to show.

This approach is different—and more flexible—than the current all-or-nothing approach used by courts like the Fourth Circuit. In *Graham*, the court stated that "an individual can claim 'no legitimate expectation of privacy' in information that he has voluntarily turned over to a third party."[156] This is because, "by 'revealing his affairs to another,' an individual 'takes the risk . . . that the information will be conveyed by that person to the Government.'"[157] The line here is clear: if you keep information to yourself, it is protected, but once you reveal it to another, you take on all risks of this information being acquired by the government. Under the reasonable assumption test, however, this revealing of data will not be the end of the inquiry. Instead, a court will have to ask what the person who provided the data would reasonably assume this data would be used for. Thus, instead of making all revealed data free from all protections, the Fourth Amendment will cover unreasonable uses of this data, with this "reasonable" analysis happening on a factual case-by-case basis.

B. Factors to Consider for a "Reasonable Assumption" Test

A number of factors could be created in order to determine how reasonable a person's assumption would be that information would not be used by law enforcement without probable cause and a warrant. First, a court could look at how sensitive the revealed information is. Information given to lending institutions and to health care providers invokes more concern about being revealed than does information spoken to a companion on a crowded train.[158] In

155. U.S. CONST. amend. IV.

156. *Graham*, 824 F.3d at 427 (quoting *Smith*, 442 U.S. at 743–44).

157. *Id.* (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

158. Information given to lending institutions is covered by a federal statute that bars the disclosure of any "nonpublic personal information" without providing notice to the

comparison, CSLI is arguably not extremely sensitive standing on its own. A single data point merely shows a person's location at a given moment, which could easily be in a public place that would otherwise have few reasonable assumptions of privacy.

Second, a court could look to the complexity of the data itself before any aggregation. For this factor, the less complex the data, the more reasonably a person may assume that this data will not be used by law enforcement against them. For instance, having a conversation with or giving a map to a police informant has no protections under either the current third-party doctrine or this test, as a defendant has no reasonable assumption that a drawn map will not be used to determine her whereabouts during a crime. These complex sets of data are enough to stand on their own and require no aggregation by the government. A person has, however, a reasonable assumption that a single data point of CSLI will not be used to map out their whereabouts, as this data point is far from complete enough to be used as a GPS substitute and requires aggregation to get to this point. For instance, a consumer swiping a credit card at a store has a reasonable assumption that this data point will not be used as a collective to determine all of her shopping habits. A phone caller, furthermore, has a reasonable assumption that her phone call will not be used to track her whereabouts for months. Essentially, a person has a reasonable assumption that such singular actions will not be used to track far beyond the scope of those actions[159]—thus creating an element that addresses some of the concerns about the aggregation of non-content raised above.

consumer prior to the disclosure. *See* 15 U.S.C. § 6802(a) (2012). This personal information includes any identifying information provided to the financial institution by the consumer that results from any transaction or was otherwise acquired by the institution. *See* § 6809(4)(A). Health information is also covered under specialized security and privacy rules that limits disclosure of personal information to third parties. *See* 45 C.F.R. § 164.502(a) (2018) ("A covered entity or business associate may not use or disclose protected health information, except as permitted or required by [various Sections and Subparts of the Chapter].").

159. Discussing whether or not people should have a reasonable assumption that they will not be subject to long-term surveillance raises policy arguments about the desirability of government surveillance, privacy, and security that are beyond the scope of this Recent Development. Tellingly, however, almost sixty percent of Americans find government's monitoring of communications of American citizens to be "unacceptable." *See* Lee Raine, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/QNW7-JVKW].

It is to be noted that this factor does not protect simple, singular data points from discovery by the government. Instead, this factor must be considered in tandem with what the government is attempting to use the data for. If the data is being used for a "reasonable" purpose—to determine one's location during a singular phone call, or to determine what store a consumer was in at the time of a crime—these single data points are unprotected, as people arguably cannot have a reasonable expectation of privacy in these singular, public actions. It is only when these singular actions are used to paint larger, unrelated pictures that they begin to become outside the realm of reasonable assumptions.

Finally, a court could perhaps look at the technological ease of the acquired data at the time of collection versus law enforcement's historical abilities to gather information. This will address Justice Alito's concerns about how investigations that used to take weeks and require significant resources and manpower can now be accomplished with devices as small, cheap, and innocuous as GPS trackers.[160] More weight will likely have to go on the first two factors, as a defendant likely will reasonably assume that technological advancements will be brought to bear against them in an investigation, but considering this can act as a brake on the impacts of swift technological changes on Fourth Amendment doctrines. Additional factors may be useful and necessary for this doctrine to be fully viable, but these will provide a starting point for the reasonable assumption test.

Applied to CSLI gathering, this test would both protect the ability of the police to do their jobs while also protecting against widespread and lengthy tracking by the government. Police could still use CSLI for individual suspects, just over a much more limited length of time, to determine whether or not a party was in the area. No explicit time limit would be mandated by this reasonable assumption test; instead, the amount of time allowed would arise from the factors in the test and the underlying data. A few singular data points of highly sensitive financial interactions, for instance, would lead to a shorter reasonable time for surveillance and aggregation, as a user arguably has more of a reasonable assumption that sensitive banking actions will be kept private. Letter addressing information and CSLI may have a longer reasonable time of

160. *See* United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring).

observation, as they are more public than these banking records.[161] However, the government could still not gather significant portions of this CSLI (and other similar non-content) and aggregate it to a point beyond what a person would *reasonably* assume that information would be used for (i.e., to essentially show what the "contents" of a message would or to show detailed, long-term tracking). This would protect against the concerns raised by Justices Sotomayor and Alito in *Jones*, and would provide a constitutional limit on the aggregation of both business records and non-content. This approach would also shift away from the all-or-nothing approach to privacy that concerned Justice Marshall in *Smith*,[162] and would approach the subject with more nuance by recognizing that people may have expectations of privacy from the government even when they do interact with third parties. This reasonable assumption would have to still allow creative uses by law enforcement,[163] but even limiting the reasonable assumption test to just aggregation would provide privacy and security to citizens that the current doctrines do not. This test could be adapted to any number of other areas that involve information revealed to third parties through the third-party doctrine or to other non-content information. To avoid over-complicating the doctrine and to protect against future technological developments, this test would cover the aggregation of all such information without regard for that information's sensitivity.

161. As noted above, the Supreme Court in *Jones* declined to draw an exact line of when tracking by the government rises to the level of a search, only finding that four weeks was over that unknown line. *See supra* note 82 and accompanying text. While the factor-driven analysis of the proposed reasonable assumption test may prove to be an imperfect methodology by which to establish the exact moment in time at which a government action becomes a search, such a factor-driven analysis alleviates the need for the creation of a hard doctrinal line, which can be difficult to articulate. The difficulties with articulating a bright line for when a police action—specifically police tracking—becomes a search was evident in *Carpenter*'s oral arguments, during which counsel for Carpenter struggled to defend his proposed line of twenty-four hours. *See* Transcript of Oral Argument at 7–15, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).

162. *See* Smith v. Maryland, 442 U.S. 735, 749 (1978) (Marshall, J., dissenting).

163. For instance, law enforcement could still make reasonable inferences based on individual data points and could use these individual data points under the third-party and non-content doctrines to carry out investigations. Just because a single data point—i.e., the location from a single phone call—would not be expected to reveal incriminating evidence would not prevent the police from using it in that manner.

C. Counterarguments to the Proposed Reasonable Assumptions Test

There are certainly criticisms and weaknesses of this test, as there likely will be with any solution to the challenges brought by the interaction of technology and the Fourth Amendment. First, this test still places the burden on individual courts and judges to make difficult, fact-based decisions, which was one of the significant concerns about using the Mosaic Theory for the aggregation of data.[164] However, the inquiry for judges will be different under this approach. Instead of looking at aggregated data to attempt to draw a line for every search, a judge will merely look to see whether or not the aggregated data is being used in a way that is different than how a reasonable person would reasonably assume this data would be used. Instead of trying to draw lines in shifting sands, judges would just have to carry out a reasonableness test.

One of the more significant criticisms is that this approach would make life harder on law enforcement.[165] This is unfortunately true, as the test would protect data from police discovery without a warrant that they can currently access without probable cause. On the other hand, the Fourth Amendment exists for the protection of the people to be secure in their papers and effects, not to make law enforcement easy. This may limit creative detective work that uses the aggregation of seemingly insignificant data points to create a picture of a potential threat to society. However, the chilling effect claimed by detractors is likely not as intense as claimed. For instance, a potential defendant has a reasonable assumption that a single IP address of an extremist website that he visits will be noticed.[166] He has a reasonable assumption that his call to a criminal organization will be noticed, and a reasonable assumption that law enforcement will spot his departure from a business commonly known as a front for a criminal enterprise. He does not, however, have a reasonable assumption that all of these data points will be used in combination to paint him a criminal, but at

164. *See* Kerr, *supra* note 73, at 346–47.

165. *See* Kerr, *supra* note 14, at 575–77. In Professor Kerr's vision, a world without the third-party doctrine would allow criminal parties to remain at home in a "bubble of Fourth Amendment protection," thus planning their crimes through channels—such as internet searches and phone calls—that police could not access. *See id.* at 576. Essentially, criminals could remain at home and work through remote agents and never be subject to observation because of a lack of third-party doctrine. *See id.* at 575.

166. *See, e.g.*, Olivia Solon, *Google's Ad Tracking is as Creepy as Facebook's. Here's How to Disable It*, THE GUARDIAN (Oct. 21, 2016, 6:48 PM), https://www.theguardian.com/technology/2016/oct/21/how-to-disable-google-ad-tracking-gmail-youtube-browser-history [https://perma.cc/N8MV-55UY].

this point a prudent person would almost certainly believe that evidence of a crime may be found in this person's home, on his phone, or on his person—thus, probable cause has been met, and a resulting warrant can allow law enforcement to gather all of the information it needs.

D. Impact on the Current Third-Party Doctrine and Content/Non-Content Distinction

While this rule would overturn established precedent that finds no expectation of privacy in voluntarily conveyed information,[167] it would not entirely overthrow the current doctrine.[168] A rule of this sort would protect against what society is most likely to find unreasonable—the aggregation of data into a detailed picture of a defendant's life that would allow the government to essentially establish guilt without ever seeking a warrant.[169] This aggregation would certainly make life simpler for the government to find and stop criminals, which is of course a worthy goal in and of itself. However, with any government power comes the potential for abuse, and granting the government the power to gather limitless non-content and third-party data could, when combined with the revealing effects of aggregation, essentially create a system of continuous and invasive government surveillance.[170] The Fourth Circuit may have sought a "sturdier" constitutional distinction[171] than what is proposed here, but the fact of the matter is that a line must be drawn somewhere before modern technology further undermines Fourth Amendment jurisprudence. Whether this means the adoption of the reasonable assumption test or some other restriction of the scope of data gathering or its aggregation could be a question for the courts or

167. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc) (applying the *Smith* third-party doctrine).

168. *See id.* at 433 (describing how content of messages is protected, but non-content is not).

169. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

170. For a pertinent discussion of the interaction between the Fourth Amendment and the NSA's large-scale metadata surveillance program, see generally Joseph D. Mornin, *NSA Metadata Collection and the Fourth Amendment*, 29 BERKELEY TECH. L. J. 985 (2014).

171. *See Graham*, 824 F.3d at 434 (stating how, under the defendant's argument, phone numbers dialed, dates and times of the call, and the source of the call would all be unprotected, while the cell towers used would be, and how "[c]onstitutional distinctions are made of sturdier stuff").

Congress, who, as the Fourth Circuit discusses, plays a large role in this process as well.[172] Either way, some sort of action is needed.

One final consideration is that the *Graham* verdict did not turn on the cell phone data at all—there was already other evidentiary information that connected the defendants to the crime scene that had been gathered under a warrant before the acquisition of the CSLI from the cell phone company, including clothing that matched clothes worn at the crime scene.[173] This is a key point, as increasing the evidentiary standard to probable cause for aggregation of non-content would not withhold evidence of crimes from the authorities entirely. Instead, it would merely protect the aggregated data until the government could show "probable cause," which is what the Constitution requires.[174] Furthermore, this is a standard that the police in *Graham* and *Carpenter* would likely have met through other police work.[175] For example, the police in *Graham* had gathered information and other evidence through search warrants—in particular, clothes found in the defendants' homes that matched those worn by the robbers at the crime scene[176]—that would have likely made a reasonable person believe that evidence of a crime (i.e., the location of the criminals near the crime scene) would be located in the CSLI. Until the point that law enforcement has gathered enough of such information for probable cause, however, people should be able to rest assured that their non-content data and information will not be so aggregated that the government will be able to clearly see the most intimate details of their lives, be that their long-term location, their health, or any number of other sensitive details.

172. *Id.* at 440 (Wilkinson, J., concurring) (noting that "[t]hroughout our history . . . it has been Congress that has taken the lead in . . . balanc[ing] the need for a new investigatory technique against the undesirable consequences of any intrusion on constitutionally protected interests in privacy." (alterations in original) (quoting Dalia v. United States, 441 U.S. 238, 264 (1979) (Stevens, J., dissenting))). Despite this note in the *Graham* concurrence that legislative solutions are often used to resolve conflicts between new techniques and constitutional interests, it is quite possible that the Supreme Court will be the source of a new test or focus when *Carpenter* is decided in 2018.

173. *See* United States v. Graham, 796 F.3d 332, 340–41 (2015), *aff'd on other grounds*, 824 F.3d 421 (4th Cir. 2016) (en banc).

174. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing . . . the persons or things to be seized.").

175. *See* Graham, 796 F.3d at 340–41. In *Carpenter*, police based their court orders off of a given confession by one of those involved in the robbery. *See* United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

176. *Graham*, 796 F.3d at 340.

CONCLUSION

The Fourth Circuit in *Graham* itself expressed a reservation for the doctrine it was upholding and broadening, saying that if it had a "clean slate," it might protect these large quantities of information,[177] but that it was bound by Supreme Court precedent.[178] These reservations are further evidence not to avoid the problems posed by the aggregation of this data to record sensitive information about individuals over time. The Fourth Circuit made a mistake when it quickly dismissed CSLI as non-content without addressing the great concerns that arise from its aggregation.[179] The court argued that society has no expectation of privacy when third parties maintain records, even when that data may be aggregated so as to reveal sensitive information similar to that of pervasive government surveillance.[180] However, this will be no small comfort to private citizens when the government can, without a warrant, look through all of the data gathered by the multitudes of third-party actors who will have access to their lives to build an intimate, detailed picture of one's health, travels, finances, sleep schedules, contacts, internet history, and purchases.[181] At this point, once again, the question must be asked: would the government even need a warrant?

The answer to this disquieting question should be an unequivocal yes. There will certainly be potential difficulties in the application of a reasonable assumptions test, both in application and in the change in precedent such a new test would create. However, courts should nevertheless hold that all of this non-content data, be it CSLI, health data, or messages from one's smart refrigerator,[182] cannot be aggregated so as to approach a level of intimacy similar to that which would be acquired by the acquisition of the contents of private communications and that goes beyond the reasonable assumption regarding the way such data will be used. This will not forbid the government from ever accessing this information; instead, it will merely provide for the reasonable protection of society's

177. *See* United States v. Graham, 824 F.3d 421, 436 (4th Cir. 2016) (en banc).

178. *See id.* at 437–38.

179. *See id.* at 434.

180. *See id.* at 435 (distinguishing *Jones* as one of impermissible *government* tracking versus that of *third party* record-keeping in *Graham*).

181. *See* United States v. Davis, 785 F.3d 498, 536 (Martin, J., dissenting) (describing the multitude of ways that third-party actors such as Google, Facebook, and Amazon could acquire potentially discoverable information); Bajarin, *supra* note 107.

182. *Family Hub Refrigerator*, SAMSUNG.COM, http://www.samsung.com/us/explore/family-hub-refrigerator/ [https://perma.cc/FHV3-YJ5U].

constitutional rights under the Fourth Amendment, and it will give courts and citizens a reasonable test to use moving forward into an ever more closely connected future.

JAMES G. MCLEOD**

** My thanks must first go to Eric Goodheart, my editor, for all of his patience and advice during the editorial process, as well as to all of the Volume 96 Board for their guidance throughout the year. Secondly, I would like to thank Professor Joe Kennedy for his thoughtful comments and feedback on this piece, as well as all of the hard work my friends Tara Summerville, Alexa Voss, and the rest of the Volume 97 Staff graciously put in to help pull this piece together. I am also forever grateful and thankful for my sister Emma and for my parents John and Beth for their unconditional love, support, and encouragement.