Science and Technology Law Review

Volume 20 | Number 1 Article 7

2017

You Can Run but You Can't Hide: Cell Phone Tracking Data Do Not Receive Fourth Amendment Protection

Merissa Sabol
Southern Methodist University, msabol@smu.edu

You Can Run but You Can't Hide: Cell Phone Tracking Data Do Not Receive Fourth Amendment Protection

*Merissa Sabol**

I. INTRODUCTION

As the world becomes more technologically advanced, courts increasingly face issues with applying traditional legal rules to complex electronic device cases. In *United States v. Graham*, the Fourth Circuit was no exception. The Fourth Circuit was recently forced to determine if the government invaded an individual's Fourth Amendment rights when it obtained, from a third party, historical cell-site location information (CSLI), which can be used to deduce "the location of a cell phone use."[1]

When making and receiving phone calls and text messages, the user generates a CSL signal. The signal is then transmitted from the phone to a cell tower to complete the call or text. The Fourth Circuit erroneously held that the government did not violate the Fourth Amendment when, without a warrant, it obtained 221-days' worth of CSLI.[2]

The court reasoned that the defendants did not have a reasonable expectation of privacy in the data because: (1) direct cell phone surveillance is distinguishable from acquiring information from a third party; (2) Supreme Court precedent and fellow appellate courts' rulings supported the holding; and (3) the data was voluntarily conveyed according to the third-party doctrine.[3] This case note criticizes the court for not thoroughly and specifically defining what it means to voluntarily convey information. Moreover, the court placed too much emphasis on the third-party doctrine instead of the Fourth Amendment's touchstone analysis that pertains to reasonableness. In a world dominated by advanced sensory data and technology, the Fourth Circuit has created dangerous precedent in light of growing security and policy concerns.

II. BACKGROUND

After a nine-day joint trial in 2015, a jury convicted Aaron Graham and Eric Jordan of several offenses arising from a series of armed robberies that occurred between January 17 and February 5, 2011.[4] On the last day of the

---

* Merissa Sabol is a 2018 candidate for a Juris Doctor from SMU Dedman School of Law. She received a Bachelor of Arts in Political Science from Baylor University.

1. United States v. Graham, 824 F.3d 421 (4th Cir. 2016) [hereinafter *Graham II*].

2. *Id.* at 424–25.

3. *Id.*

4. United States v. Graham, 796 F.3d 332, 339 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015), and *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016) [hereinafter *Graham I*].

spree, Graham and Jordan were arrested for the robberies.[5] After lead investigator Chris Woerner noticed several similarities between the robberies, he prepared and executed search warrants for Graham's residence, Jordan's residence, and the get-away pickup truck.[6] The searches recovered various items, including two cell phones.[7] Warrants for the phones were successfully obtained, and Detective Woerner matched each phone number to the ones previously shared by the defendants.[8]

In preparation for trial, the government requested cell phone information from the service provider, Sprint/Nextel, through two court orders for the disclosure of historical CSLI for calls and texts transmitted to and from both phones.[9] The government submitted a broad application for information from July 1, 2010 through February 6, 2011, a 221-day span.[10] The application was granted and the government used the recovered CSLI at trial to place Graham and Jordan near the banks at the time the armed robberies occured.[11]

Graham and Jordan filed several pre-trial motions, including a motion to suppress the CSLI data obtained by the government from Sprint/Nextel on Fourth Amendment grounds.[12] The U.S. District Court of Maryland denied the motion to surpress, and the case proceeded to trial.[13] Ultimately, a jury returned guilty verdicts for both defendants on all counts.[14] After the District Court denied the defendants' motion for re-trial, the defendants appealed to the Fourth Circuit Court of Appeals.[15] In its first hearing, the Fourth Circuit held that acquiring CSLI without a warrant was a violation of the defendants' Fourth Amendment rights.[16] The government subsequently moved for; and was granted, a rehearing en banc.[17] The Fourth Circuit's second hearing, and the subject of this case note, affirmed the defendants' convictions and held that there was not a Fourth Amendment violation.[18]

5. *Id.* at 339–40.
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Graham I*, 796 F.3d at 341.
11. *Graham II*, 824 F.3d at 424.
12. *Graham I*, 796 F.3d at 341.
13. *Id.*
14. *Id.* at 342.
15. *Id.*
16. *Graham II*, 824 F.3d at 424.
17. *Id.*
18. *Id.* at 424 n.1.

III. PRIVACY LAW

A. The Fourth Amendment

The issue before the court was whether obtaining the historical CSLI records qualified as a Fourth Amendment search.[19] The Fourth Amendment safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[20] A search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.[21] Inquiry into whether such a search occurred begins by identifying the nature of the challenged state activity.[22] Here, the activity was the government's procurement of historical CSLI records from Sprint/Nextel.[23]

B. The Third Party Doctrine

The third-party doctrine provides an exception to the expectation of privacy granted by the Fourth Amendment.[24] The U.S. Supreme Court declared that an individual does not receive the protection of the Fourth Amendment in information he voluntarily turns over to a third party,[25] even when the information is revealed assuming that it will be used only for a limited purpose and the confidence between the parties will not be betrayed.[26] By voluntarily revealing private affairs, the individual risks that the information will be given to the government.[27] Thus, an individual cannot expect the Fourth Amendment to protect information voluntarily disclosed to third parties because society does not recognize a subjective expectation of privacy in the information as reasonable.[28]

C. The Stored Communications Act

To retrieve historical CSLI records from a third party, the government must follow the Stored Communications Act (SCA).[29] To gain access to non-content records, the SCA mandates that the government: (1) obtain a warrant

19. *Id.* at 425.

20. U.S. CONST. amend. IV.

21. *Graham II*, 824 F.3d at 425 (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

22. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979)).

23. *Id.*

24. *Id.*

25. *Id.* (quoting *Smith*, 442 U.S. at 741).

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

27. *See Graham II*, 824 F.3d at 427 (quoting *Miller*, 425 U.S. at 443).

28. *See id.* (quoting *Smith*, 442 U.S. at 743).

29. *Id.* at 426.

by a court of competent jurisdiction;[30] (2) use an administrative subpoena or trial subpoena if prior notice was given to the subscriber or customer;[31] or (3) obtain a court order following Section 2703(d).[32] Here, the government chose to secure a court order through the third option.[33] Abiding by the Section 2703(d) procedure for a court order, the government had to provide "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation."[34] On this point, Graham and Jordan argued that the SCA violates the Fourth Amendment by permitting the government to collect private information.[35]

IV. HOLDING AND RATIONALE

The Fourth Circuit found that the government's acquisition of CSLI from Sprint/Nextel did not constitute a search; thus it did not violate the Fourth Amendment.[36] The court's rationale had many bases, including: (1) distinguishing direct surveillance and acquiring information from a third party; (2) Supreme Court precedent and fellow appellate court rulings; and (3) the third-party doctrine.[37]

A. Direct Surveillance Distinguished

The Fourth Circuit began its analysis by distinguishing direct government surveillance and acquiring information from a third party.[38] Relying on three Supreme Court cases, defendants argued that there is always an invasion of an individual's reasonable expectation of privacy when the government uses technological devices to track one's movement.[39] The court disagreed and found that the government did not engage in tracking or direct surveillance of the defendants.[40] Although the government might have been able to deduce location information, the CSLI data obtained did not enable the government to specifically locate either defendant because it could only

30. 18 U.S.C. §§ 2703(b)(1)(A), (c)(1)(A) (2012).

31. *Id.* § 2703(b)(1)(B)(i).

32. *Id.* §§ 2703(b)(1)(B)(ii), (c)(1)(B).

33. *Graham II*, 824 F.3d at 439 (Wilkinson, J., concurring).

34. 18 U.S.C. §§ 2703(c), (d).

35. *Graham II*, 824 F.3d at 426.

36. *Id.* at 424.

37. *Id.* at 424–38.

38. *Id.* at 426.

39. *See id.*; *see also* United States v. Jones, 132 S. Ct. 945, 949 (2012); Kyllo v. United States, 533 U.S. 32–33 (2003); United States v. Karo, 468 U.S. 705, 714–15 (1984).

40. *Graham II*, 824 F.3d at 426.

determine a four-square-mile area,[41] whereas direct surveillance would have provided an exact pinpoint location.

B. Precedent

Then, the Fourth Circuit asserted that Supreme Court precedent from *Smith v. Maryland* was controlling.[42] Similar to *Smith*, the defendants "unquestionably exposed" the CSLI information transmitted from their phones to Sprint/Nextel through their equipment,[43] and making or receiving a call or text are activities within the ordinary course of cell phone ownership.[44] By giving the CSLI to Sprint/Nextel, the defendants assumed the risk that Sprint/Nextel would disclose the data to the government.[45]

The court bolstered its reasoning by relying on controlling law from fellow appellate courts.[46] The Third, Fifth, Sixth, and Eleventh Circuit Courts hold that there is no reasonable expectation of privacy in CSLI data obtained by the government via a SCA Section 2703(d) order.[47] The defendants' arguments lacked support from "relevant authority and would place [the Fourth Circuit] in conflict with the Supreme Court and every other federal appellate court to consider the question"—a position this court was unwilling to take.[48]

C. Third Party Doctrine

Next, the defendants argued that the third-party doctrine was inapplicable because a cell phone user does not own the CSLI to voluntarily convey information and, even if he or she did, revealing the information is compelled, not voluntary.[49] The Fourth Circuit rejected this argument because defendants, "misapprehended the nature of CSLI, improperly attempted to redefine the third-party doctrine, and [relied] on a long-rejected factual argument."[50]

The court found that CSLI is conveyed by the user, to the service provider, through information generated by making and receiving calls or texts through the phone.[51] For a service provider to generate a CSLI record, the

41. *Id.* at 426 n.3.

42. *Id.* at 425.

43. *Id.* at 427; *see* Smith v. Maryland, 442 U.S. 735, 744 (1979).

44. *Graham II*, 824 F.3d at 427.

45. *Id.* at 427–28.

46. *Id.* at 428, 436–37.

47. *Id.* at 428.

48. *See id.* at 429.

49. Supp. Brief of Defendant-Appellants at 10–11, *Graham II*, 824 F.3d 421 (4th Cir. 2016) (No. 12-4659) (en banc).

50. *Graham II*, 824 F.3d at 429.

51. *Id.*

transmission of information must occur between the phone and cell tower.[52] The conveyance is voluntary because a user's location is recorded whenever he voluntarily makes or receives calls and texts through the provider's network.[53] While users do not directly inform service providers of which cell tower to use, voluntariness is inherent in the nature of the purchase and service agreement to provide cell phone reception.[54]

Further, the defendants tried to redefine the third-party doctrine by asserting that it is inapplicable because users do not actively choose to share CSLI information.[55] However, the court held that this requirement is unfounded in federal case law.[56] Many federal rulings permit the government to acquire third-party records, even when individuals do not actively choose to share historical CSLI.[57] If changed to an "actively choosing to share" rule, "then any effort to acquire records of incoming phone calls would constitute a search protected by the Fourth Amendment" because only the user that dialed the call actively chose to share the information.[58]

The defendants also inappropriately relied on a long-rejected factual argument and case law involving the content of communications, as opposed to non-content communications.[59] Defendants argued that conveying CSLI information is involuntary because they must either produce CSLI or opt out of society.[60] Dissenting justices have made similar arguments in prior cases, but the court here found that reliance on those opinions was misplaced.[61]

Moreover, defendants relied on case law involving disputes over the *contents* of the communications (i.e., information contained in the communication) as opposed to *non-content* information (i.e., information that enables service providers to transmit the content).[62] CSLI is non-content because it specifically identifies the equipment used to route calls and texts.[63] The majority admitted that security concerns can arise from the aggregation of non-

52. *Id.*

53. *Id.* at 430.

54. *Id.*

55. *Id.* at 431 (quoting Redacted Brief of Defendant-Appellants at 30, *Graham II*, 824 F.3d 421 (4th Cir. 2016) (No. 12-4659, 12-4825)).

56. *Graham II*, 824 F.3d at 431.

57. *Id.*

58. *Id.*

59. *Id.* at 432.

60. Supp. Brief of Defendant-Appellants, *supra* note 50, at 11.

61. *Graham II*, 824 F.3d at 433; *see* United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting); Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

62. *Graham II*, 824 F.3d at 433.

63. *Id.*

content routing information, but it would "blink[ ] at reality" to find that CSLI rises to the level of content needed for Fourth Amendment protection.[64]

Finally, defendants contended that the amount of information obtained—seven months of records—was a search.[65] Relying on the fact that the third-party doctrine contains an intrinsic assumption that quantity does not matter, and because the CSLI data was voluntarily conveyed, the court held that the "very act of disclosure negated any reasonable expectation of privacy, regardless of how frequently that disclosure occurred . . . ."[66] Moreover, the court opined that the legislative branch is far better positioned to adjust privacy protections as technology develops.[67] The Supreme Court may revisit the third-party doctrine one day, but the Fourth Circuit maintained that it was "bound by the contours" of the current third-party doctrine.[68]

V. CONCURRING AND DISSENTING OPINIONS

A. Judge Wilkinson's Concurring Opinion

Judge Wilkinson's concurring opinion emphasized his concern that requiring probable cause and a warrant to obtain CSLI data would "needlessly supplant" a congressional standard with a judicial one.[69] Section 2703(d) already mandates the requirements for a valid court order and provides a standard of reasonable suspicion.[70] Judge Wilkinson supported the majority's holding because to accept the defendants' approach would overturn Supreme Court precedent and destroy congressional efforts to balance privacy and law enforcement interests.[71]

Developing constitutional meaning is not the sole responsibility of the judiciary but instead, a "collaborative enterprise among the three departments of government."[72] Moreover, when Congress has weighed in on the requirement of reasonableness within the context of the Fourth Amendment, a certain degree of deference should be given to the legislature given its greater access to expert opinions, better positioning for legal consistency, and the preservation of democratic legitimacy to a highly controversial area rife with

64. *Id.* at 434.

65. *Id.*

66. *Id.* at 435–36.

67. *Graham II*, 824 F.3d at 436.

68. *See id.* at 437.

69. *Id.* at 438 (Wilkinson, J., concurring).

70. *Id.* at 439.

71. *Id.*

72. *Id.*

criminal motivations.[73] In sum, Judge Wilkinson found it unnecessary to depart from a "carefully tailored scheme."[74]

B. Judge Wynn's Partial Dissent

Judge Wynn wrote a partial dissent affirming the defendants' convictions but objecting to violations of the Fourth Amendment.[75] He analyzed the Supreme Court's use of voluntary conveyance through case law.[76] The two elements of voluntary conveyance are knowledge of the particular information and an action submitting the information.[77] A cell phone user is likely unaware that any CSLI data is being transmitted; that he is conveying it; that his service provider is collecting and storing the data; and that specific cell phone towers are routing his calls and texts.[78] Thus, Judge Wynn found that user knowledge was absent.[79]

Furthermore, "CSLI is purely a function and product of cell phone technology, created by the provider's network when a cell phone call connects to a cell site."[80] The network automatically generates CSLI when the phone receives a call, whether or not the user actually answers or participates.[81] "Because a user neither possesses knowledge of the information nor actively submits the information," he or she could not have voluntarily conveyed location information.[82]

In application, because CSLI data is not voluntarily conveyed, Judge Wynn argued that these circumstances cannot be evaluated purely by the third-party doctrine.[83] A proper analysis should include an independent evaluation of the quality and quantity of data acquired and would ask whether the government "violated a subjective expectation of privacy that society recognizes as reasonable."[84] Although CSLI may not be able to pinpoint a direct address like a GPS, the quantity of cell site points collected over 221 days is

73. *Graham II*, 824 F.3d at 440.

74. *Id.* at 439.

75. *See id.* at 441 (Wynn, J., dissenting).

76. *See id.* at 442.

77. *Id.* at 443.

78. *Id.* at 445.

79. *Graham II*, 824 F.3d at 445 (Wynn, J., dissenting).

80. *Id.* (quoting Commonwealth v. Augustine, 4 N.E.3d 846, 862 (2014)) (internal quotations omitted).

81. *Id.*

82. *Id.* at 446 (quoting *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010)).

83. *Id.* at 446.

84. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001).

nearly eight times greater than that determined unconstitutional in *Jones*.[85] Judge Wynn reasoned that the vast quantity of data gathered provided extensive details about the defendants' locations, infringing on their reasonable expectation of privacy under the Fourth Amendment.[86]

Judge Wynn also raised future policy concerns implicated by the majority's decision.[87] He stated that the rule was too broad because as technology allows for a proliferation of smaller and smaller cell sites or the advent of smartphone "pinging," the outcome stagnates.[88] Because the majority did not take into consideration the preciseness of the data collected, the holding is inadaptable and inflexible as technology becomes more sophisticated.[89]

VI. CRITIQUE OF THE COURT'S RATIONALE

A. The Components of the Third-Party Doctrine

The Fourth Circuit's justification for relying on the third-party doctrine is particularly troublesome as the crux of the analysis—voluntary conveyance—is frustratingly vague. It is indisputable that the CSLI was actually conveyed. Instead, the analysis hinges on whether or not it was *voluntarily* conveyed. The true legal meaning of "voluntary" necessitates a thorough analysis of its uses and surrounding factual circumstances. The dissent's argument is the most compelling because of its thorough investigation into case law and its determination of what it truly means when someone voluntarily conveys data.

For example, in *United States. v. Bynum*, the Fourth Circuit held that the third-party doctrine applied to subscriber information when an individual typed his name, email address, phone number, and physical address into a form and then submitted the information to a service provider to secure internet access.[90] There, the defendant not only had knowledge of the information he provided, but he also knew he was releasing that information to the service provider, and he affirmatively acted in doing so.[91] Moreover, in *United States v. Forrester*, the Ninth Circuit held that the third-party doctrine applied to the IP addresses of visited websites.[92] When an internet user typed a URL—which is tied to a single IP address—into a web browser and hit

85. *Graham II*, 824 F.3d at 447–48 (Wynn, J., dissenting).

86. *Id.* at 448.

87. *Id.*

88. *Id.* at 448–49.

89. *Id.* at 448.

90. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

91. *Id.*

92. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

"Enter," the user knew the web address being used and actively submitted the information to get to that website.[93]

Here, the defendants never interacted with the CSLI function in the same way one types in a URL to go to a website destination or subscriber information to access the Internet. In all of the cases relied on by the majority, there were many data pieces compiled into records and a discrete action behind each piece of data.[94] But in *Graham*, no discrete action on behalf of the defendants occurred. In other words, there was not the same knowing disclosure of CSLI data to phone companies because cell phone users never affirmatively disclosed their location to the service provider to make a call.[95] The defendants cannot choose the cell tower that receives the CSLI signal, which carries out the desired activity. Dialing a phone number or sending a text message and expecting either to be sent because of an intrinsic, discrete function of cellular service is distinct from the process of using a specific URL code to visit a specific website. Further, it is likely that the defendants had absolutely no knowledge that their cell phones were transmitting historical CSLI as they received and made calls or text messages. The defendants also likely had no knowledge that Sprint/Nextel was collecting and saving the data.

Moreover, it is illogical to conclude that because a user voluntarily purchased the equipment and signed a service agreement, he also voluntarily agreed and actively conveyed private personal data through his rightful ownership and use of the device. Voluntarily agreeing to own the hardware should not mean that any and all data naturally and involuntarily transmitted through it to a third party is an intentional abandonment of all privacy expectations. For example, simply because one owns a computer needed to utilize purchased internet services, does not justify the conclusion that the individual has divested himself of all reasonable expectations of privacy by using the required tools for connection. Nonetheless, the majority uses this argument as justification for eliminating all Fourth Amendment protection.

Consumers have devices that are connected to and send information to a number of different entities, and consumers do not realize that the device is connected or that it is collecting private information.[96] The majority's expansive holding fails to help future courts distinguish between information an individual voluntarily conveys and information electronic devices automatically record, generate, and transmit to third parties.[97] Accepting the dissent's

93. *Id.*

94. *Graham II*, 824 F.3d at 443 (Wynn, J., dissenting).

95. United States v. Davis, 785 F.3d 498, 534–35 (11th Cir. 2015) (Martin, J., dissenting).

96. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 90 (2014).

97. *Graham II*, 824 F.3d at 446 n.8 (Wynn, J., dissenting).

thorough analysis of what it means to voluntarily convey information would provide latitude for a court to truly analyze the knowledge and active conduct of the user. The failure to distinguish between something that is intentionally chosen and voluntarily conveyed versus something that is forcibly conveyed leaves an expanding technological era with an outdated view of information conveyance.

B. Re-Focusing the Analysis of *Graham II* Towards the Two-Part *Katz* Test

The majority's opinion relies heavily on the third-party doctrine as well as content and non-content designations. As technology has advanced and society's reliance on it has grown, the extent of information exposed to third parties has increased considerably since *Miller* and *Smith* (cases to which the majority gives significant weight).[98] In *Jones*, Justice Sotomayor stated:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[99]

The Fourth Amendment makes clear that the touchstone of the analysis is reasonableness. *Katz v. United States* is the cornerstone case in which the Supreme Court established the reasonable-expectation-of-privacy test in determining whether a Fourth Amendment search had occurred.[100] The test is two-fold: (1) whether the individual manifested a subjective expectation of privacy; and (2) whether that expectation of privacy is one society would recognize as reasonable.[101]

This test, as opposed to the third-party doctrine or the content or non-content designation, can provide the discretion necessary to analyze these issues as technology progresses. If the touchstone of the Fourth Amendment analysis is reasonableness, then each case should be analyzed according to this two-part test. Simply because a user voluntarily conveys information to a third-party should not mean that he is automatically without Fourth Amendment protection. Furthermore, having to draw a line in a mountain of data to determine what is non-content and what is content leaves little structure for future application of the law because the list would be endless.

98. *Davis*, 785 F.3d at 538 (Martin, J., dissenting).

99. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

100. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967).

101. California v. Ciraolo, 476 U.S. 207, 211 (1986).

Moreover, information that might be deemed as non-content in a singular occurrence could be viewed as content in the aggregate. The *Katz* test allows for flexibility, while applying a rigid rule to ever-evolving fact scenarios by investigating the truth of what an individual expects to keep private. Surveillance data "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about his familial, political, professional, religious, and sexual associations."[102] The aggregation of CSLI data points could equally convey what the contents of one letter, email, phone call, or text message could reveal. Relying more heavily on the established *Katz* test will provide a more accurate and protective analysis of what one expects to keep private. Ultimately, this will secure the greatest amount of constitutional protection.

C. Future Implications for Data Transmitted and the Reasonable Expectation of Privacy

The Fourth Circuit's decision in *Graham* is especially problematic in the context of security and one's expectation of privacy. Technology is quickly advancing and growing more and more pervasive, especially in the realm of electronic sensors. For instance, the Breathometer is a device that plugs into the headphone jack of your smartphone and contains an ethanol sensor to estimate blood alcohol content from one's breath.[103] However, the manual never mentions a privacy policy governing the data generated by the device or where the information is stored.[104] The privacy policy is actually on the company's website, at the bottom of the webpage, in a small link, which then informs the user that one's blood-alcohol test results are stored "*indefinitely* in the cloud, cannot be deleted by the user, [and] may be disclosed in a court proceeding if necessary . . . ."[105] The potential ramifications that data can have on a user's life are vast: employment, criminal liability, obtaining insurance, to name a few.[106] The Breathometer is just one example of the thousands of electronic sensors that capture incredibly nuanced data about our personalities, habits, tastes, and behavior.

Despite the differences in data between historical CSLI data and blood alcohol content from the Breathometer, the data provided enough precise pinpoint location data to convince a jury that Graham's and Jordan's location patterns were conviction worthy.[107] Applying the majority's rule to the Breathometer sensor data would render the information stored on third party servers and clouds unprotected by the Fourth Amendment because it is non-

102. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

103. Peppet, *supra* note 97, at 87.

104. *Id.* at 89–90.

105. *Id.* at 90 (emphasis added).

106. *Id.*

107. *Graham II*, 824 F.3d 421, 440 (4th Cir. 2016).

content and is voluntarily conveyed by the user to a third party. Although the government may not have access to the results of the blood alcohol test, under the majority's holding, they could gather enough data to deduce frequency of use, as well as where and when you use the application. This effectively means that private health data is unprotected by the Fourth Amendment—a realm of life that society has consistently shown warrants a reasonable expectation of privacy.

VIII. CONCLUSION

The Fourth Circuit failed to accurately and fully identify what it means for an individual to voluntarily convey information under the third-party doctrine. The opinion neither used the proper Fourth Amendment analysis of reasonableness, nor fully comprehended the repercussions and impact this precedent will have on society and future courts. Although the defendants failed to convince a jury of their innocence, the Fourth Circuit should have unanimously agreed that allowing acquisition of this critical evidence was a violation of the defendants' Fourth Amendment rights. To think that this precedent could potentially govern health, fitness, and personal data transmitted through other applications on smartphones or other electronic devices shows just how broad and unwise this decision is. As the majority suggests, hopefully the legislature will assume its proper role in lawmaking and remedy the wrong created by this holding. Without a reassessment of the rule, this country is potentially left with an inflexible precedent that is slowly diluting the rights protected by the Constitution.