COMMENT

A DIGITAL DEPARTURE FOR THE FOURTH AMENDMENT'S ANALOG ANALOGIES*

TABLE OF CONTENTS

I. INTRODUCTION 15

II. UNDERSTANDING CELL-SITE LOCATION INFORMATION 17

III. FOURTH AMENDMENT PROTECTIONS AND THE THIRD-PARTY DOCTRINE 19
- *A. Of Physical Invasions and Voluntary Conveyance* 20
- *B. Expectations of Privacy: A Pivot Towards a Normative Jurisprudence* 22
- *C. Modern Third-Party Doctrine* 25
- *D. Third-Party Doctrine and CSLI* 29

IV. THE MODERN COURT'S FOURTH AMENDMENT PERSPECTIVE 31
- *A. Third Party Doctrine and Modern Technologies in the Jones Court* 31
- *B. Jones's Circuit Court Impact* 33

V. CONCLUSION 36

I. INTRODUCTION

Every several seconds, your cell phone pings a nearby cell tower.[1] With each phone call made, text message received, or

* J.D. Candidate, University of Houston Law Center, 2017.

This Comment received the Jackson & Walker LLP Award for Most Outstanding Paper in the Area of Media Law. Special thanks to Professor D. Theodore Rave and the editors of HLR*e*.

1. United States v. Graham, 796 F.3d 332, 350 (4th Cir. 2015).

webpage browsed, your cell phone communicates with the cellular network.[2] And for every packet of information sent or received, service providers retain a record of your cell phone's location.[3] In turn, law enforcement agents are able to retrieve this information from your service provider without probable cause or a warrant because the phone-tower interaction is a voluntary conveyance of your location to a third party.[4]

This unchecked exercise of executive power threatens the individual privacy of all cell phone users and the protections of the Fourth Amendment.[5] Regardless, the U.S. Supreme Court has consistently held that an individual, whenever she voluntarily conveys information to a third party, no longer retains any reasonable expectation of privacy that the Fourth Amendment would otherwise protect.[6] Recent circuit court decisions have unjustifiably expanded Fourth Amendment jurisprudence in order to capture cell phone location information.[7] All during a time when public opinion is firmly in favor of curtailing, not enlarging, the surveillance state.[8]

This Comment surveys recent case law applying the Third-Party Doctrine to cell-site location information ("CSLI"), which is the record of locations extrapolated from the signals exchanged between cell phone and cell tower. Although the majority of circuit

---

2. *Graham*, 796 F.3d at 343; *see also* United States v. Davis, 754 F.3d 1205, 1210–11 (11th Cir. 2014).

3. *Graham*, 796 F.3d at 343, 350; *Davis*, 754 F.3d at 1210–11; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 708–09 (2011), http://digitalcommons.law.umaryland.edu/mlr/vol70/iss3/6 (discussing how, at minimum, the duration, registration, and location data is recorded and how this information can be used to track cell phone users).

4. *See In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 611–15 (5th Cir. 2013) (applying the Third-Party Doctrine in the cell-cite location information ("CSLI") context in order to circumvent the Fourth Amendment's warrant requirement).

5. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

6. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979);United States v. Miller, 425 U.S. 435, 440 (1976).

7. *See infra* notes 74–99 and accompanying text (examining the evolution of Fourth Amendment jurisprudence in the modern era).

8. Recent research on public opinion demonstrates that "82% of adults 'feel as though the details of their physical location gathered over a period of time' is 'very sensitive' or 'somewhat sensitive.'" United States v. Davis, 785 F.3d 498, 538–39 (2015) (en banc) (Martin, J., dissenting) (citing MARY MADDEN, PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST–SNOWDEN ERA 34 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf); *see also* Jim Finkle, *Solid Support for Apple in iPhone encryption fight: poll*, REUTERS (Feb 24, 2016, 2:47 pm), http://www.reuters.com/article/us-apple-encryption-poll-idUSKCN0VX159 (noting a near majority of Americans supported Apple's decision to defy a court to decrypt an individual's cellular data).

courts hold that CSLI falls within the Third-Party Doctrine exception to the Fourth Amendment's protections, a circuit split is developing. This Comment argues that the Court's more recent Fourth Amendment decisions signal a hesitance to extend the Third-Party Doctrine to automatically-generated digital data such as CSLI. Section II explains how cell phone technology operates and service providers collect CSLI. Section III explores the development of Fourth Amendment protections, the origins of the Third-Party Doctrine, and its application to CSLI in the circuit courts. Section IV discusses the Supreme Court's opinion *United States v. Lopez* and its impact on the lower courts regarding the interplay between the Fourth Amendment and new technologies. Section V concludes that the Third-Party Doctrine should not apply to CSLI because individuals do not voluntarily convey CSLI to a third party.

II. UNDERSTANDING CELL-SITE LOCATION INFORMATION

To fully appreciate the privacy interest associated with CSLI requires some basic knowledge about how cell phones function.[9] Whenever a cell phone powers on, it regularly identifies itself with the nearest cell site with the strongest signal.[10] This process is automatic, occurring every few seconds for smartphones.[11] Similarly, a cell phone sends additional signal data to the cell site when the phone makes a call, connects to the Internet, or sends a text message.[12] Setting aside smartphone technologies and internet connections, the call records alone can reveal an individual's location an average of every five minutes.[13] Even when the subscriber is not using the phone, this automatic process of registration still occurs, as long as the phone is on.[14] Registration is necessary in order for the service provider to "quickly locate the phone and place a call to it or from it through the nearest cell tower."[15]

When a subscriber makes or receives a call, the service provider records the identity and location of the cell site used to connect the call, surf the internet, or send a text message.[16] This automatic recording of cell phone registration data produces a log

---

9. *See generally* United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015); United States v. Davis, 754 F.3d 1205, 1210–11 (11th Cir. 2014).

10. *Graham*, 796 F.3d at 343; s*ee also Davis*, 754 F.3d at 1211.

11. *Graham*, 796 F.3d at 350.

12. *Graham*, 796 F.3d at 343; *see also Davis*, 754 F.3d at 1210–11.

13. United States v. Davis, 785 F.3d 498, 540 (11th Cir. 2015) (en banc) (Martin, J. dissenting).

14. *See Graham*, 796 F.3d at 349–50.

15. Freiwald, *supra* note 3, at 705.

16. *Davis*, 754 F.3d at 1210–11; *Graham*, 796 F.3d at 343, 350; Freiwald, *supra* note 3, at 708–09.

of all the cell sites with which the cell phone registered.[17] These location data records are typically stored in a database, where law enforcement can access and analyze them to approximate the phone's location at a given time.[18] This Comment refers to the location data which results from registration, texting, Internet use, and placing/receiving phone calls collectively as cell-site location information ("CSLI").

Admittedly, CSLI is not as accurate as GPS monitoring for creating a record of an individual's movements.[19] Regardless, CSLI still creates an incredibly detailed record of a cell phone's location and, with time, will likely surpass GPS technology in its ability to track an individual.[20] As cell phone use has grown, service providers have built increasingly more cell sites to provide service to a growing number of customers.[21] As the number of cell sites increases, the area covered by each site shrinks, so that the identity of a cell site is a more precise indicator of the phone's location.[22] In denser urban environments, CSLI can pinpoint a phone's location to "a very, very specific location, such as a floor of a building or even an individual room . . . ."[23] Smartphones have the potential to generate a near constant flow of CSLI, as most smartphone functions involve

17. *See* Freiwald, *supra* note 3, at 705–06.

18. *See Davis*, 754 F.3d at 1210–11.

19. *See* United States v. Davis, 785 F.3d 498, 515 (11th Cir. 2015) (en banc).

20. *See* United States v. Graham, 796 F.3d 332, 348 (4th Cir. 2015) ("[U]nlike GPS monitoring of a vehicle, examination of historical CSLI can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home.").

21. *See Davis*, 785 F.3d at 540 (en banc) (Martin, J., dissenting) (noting metropolitan areas have many cell towers each with a range of less than a mile and half and whose coverage area is subdivided into three to six sectors). The cell phone industry itself recognizes that due to technological limitations on the amount of data each tower can process, as demand continues to increase within densely populated areas, towers must be erected which each serve smaller geographic areas. *See* CTIA—THE WIRELESS ASSOCIATION, ANNUAL WIRELESS INDUSTRY SURVEY (2014), http://www.ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2014_graphics.pdf?sfvrsn=0 (showing that the number of cell sites in the United States nearly doubled from 2003 to 2013 while data usage increased nearly by a factor of ten in less than half that time). While CSLI may not be as accurate as GPS currently, this trend shows that its accuracy will likely increase as providers create an even denser network of cell towers in an attempt to meet demand.

22. *See Davis*, 785 F.3d at 540 (en banc) (Martin, J., dissenting); Freiwald, *supra* note 3 at 710–11.

23. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 16 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://judiciary.house.gov/_files/hearings/printers/111th/111-109_57082.pdf.

downloading data or accessing the Internet, which in turn emits location data to a cell tower.[24]

The combined effect of the frequency and increasing precision of these data points is that a subscriber, merely by carrying her cell phone on her person, unwittingly provides to her service provider a detailed account of her physical movements.[25] The government may later compel the service provider to turn over that subscriber's CLSI records under the Stored Communications Act, which does not require the government to first obtain a warrant.[26] This means that ordinary citizens' movements are being constantly monitored and recorded, and the government can obtain these records, without a warrant, thereby gaining a mountain of information most would want to keep private.[27]

III. FOURTH AMENDMENT PROTECTIONS AND THE THIRD-PARTY DOCTRINE

Despite the obvious concerns of arbitrary use of a government power to track the movements of its citizens, prosecutors have traditionally relied on the Third-Party Doctrine to introduce CSLI as evidence in criminal prosecutions. The Third-Party Doctrine denies Fourth Amendment protection to any information voluntarily conveyed to a third party.[28] The rule grew out of a string of Supreme Court decisions applying the expectation-of-privacy test established in the landmark decision *Katz v. United States*.[29] Subsequently, the Court misinterpreted prior Fourth Amendment decisions, which led to a muddying of the judicial waters and an overexpansion of the Third-Party Doctrine, which in turn created the basis for decisions holding that cell phone users do not have a reasonable expectation of privacy in CSLI.

Understanding the development of Fourth Amendment jurisprudence as the Third-Party Doctrine developed is necessary to support any attack on judicial misapplication of that doctrine. Part III.A discusses the limited protection the Fourth Amendment provided prior to *Katz*. Part III.B tracks the development of *Katz*'s normative test. Part III.C considers the Third-Party Doctrine as

---

24. *See* Freiwald, *supra* note 3, at 708–09; *see also Graham*, 796 F.3d at 350.

25. *See* Freiwald, *supra* note 3, at 709.

26. *See* 18 U.S.C. § 2703 (2011).

27. *In re* United States for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011).

28. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).

29. 389 U.S. 347 (1967); *see also Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–43.

expanded in the *Miller* and *Smith* decisions. Lastly, Part III.D traces how lower courts have applied the Third-Party Doctrine to CSLI and circumvented Fourth Amendment protection.

A. Of Physical Invasions and Voluntary Conveyance

For more than a century after ratification by the states, the Fourth Amendment (along with the rest of the Bill of Rights) was hardly ever subject to litigation or judicial inquiry.[30] Federal criminal jurisdiction began expanding significantly during the late nineteenth century.[31] As criminal defendants contested the federal government's expansion into narcotics and similar areas, Fourth Amendment questions began to flood the courts.[32] The Supreme Court narrowed the Fourth Amendment's protections against unreasonable searches and seizures to three questions: (1) what government actions constitute a search or seizure, (2) what limitations on these actions may properly qualify them as reasonable, and (3) if a government act has violated the Fourth Amendment, what is an appropriate remedy.[33] Because the third question is beyond the scope of this article, the following explores only the first two questions.

In *Olmstead v. United States*, the petitioners' expansive liquor smuggling operation resulted in a conviction for conspiracy to violate the National Prohibition Act.[34] The government obtained much of the evidence against Olmstead via wiretaps set in the telephone wires over the public streets.[35] Presented to the Court was the question of whether these wiretaps violated the Fourth Amendment's guarantee against unreasonable searches and seizures.[36] Justice Taft, after reviewing the precedents of the

---

30. *See* GORDON S. WOOD, EMPIRE OF LIBERTY: A HISTORY OF THE EARLY REPUBLIC, 1789–1815, 72 (2009) ("[T]he states ratified the first ten amendments . . . between 1789 and 1791 . . . . After ratification, most Americans promptly forgot about the first ten amendments to the Constitution. The Bill of Rights remained judicially dormant until the twentieth century.").

31. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION, 106 (1937). *See, e.g.* Interstate Commerce Act of 1887, ch. 104, 24 Stat. 379; Sherman Act, ch. 647, 26 Stat. 209 (1890).

32. *See* LASSON, *supra* 31, at 106 ("[W]ith the extension of the criminal jurisdiction of the United States over . . . narcotics and intoxicating liquors, the Fourth Amendment became one of the most . . . litigated provisions of the Bill of Rights.").

33. Peter Arenella, *Fourth Amendment*, *in* 3 ENCYCLOPEDIA OF THE AM. CONST. 1092, 1092 (Leonard W. Levy & Kenneth L. Karst, eds., 2d ed. 2000).

34. 277 U.S. 438, 455 (1928) ("[P]etitioners were convicted . . . of a conspiracy to violate the National Prohibition Act . . . by unlawfully . . . importing intoxicating liquors . . . .").

35. *Id.* at 456–57 ("The information [against petitioners] was largely obtained by intercepting messages[] . . . along the ordinary telephone wires[] . . . in the streets near the houses.").

36. *Id.* at 455 ("[T]he hearing should be confined to the single question whether the

court, concluded that the evidence in question did not violate the Fourth Amendment because no physical entry of the defendant's property had occurred.[37] Before determining a violation had not occurred, the Court briefly entertained an analogy between wiretaps and precedents holding sealed letters and packages were protected from search and seizure by the Fourth Amendment.[38] Taft rejected this analogy on textualist grounds because the language of the amendment addresses a person's *papers*, thereby proscribing searches of letters but offering no similar protections to telephone conversations.[39]

Though the *Olmstead* majority was not comfortable recognizing individual privacy interests under the Fourth Amendment beyond what the language expressly authorized, Justice Brandeis dissented. He argued the Constitution "conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[40] With time, this formulation of a constitutional right to privacy would prevail not only in Fourth Amendment jurisprudence, but also in substantive due process.[41] As Brandeis's viewpoint gained favor, the Court slowly realized the Fourth Amendment guaranteed individuals some amount of protection beyond physical intrusions.[42]

Before reaching this conclusion, the Court spent the intervening decades crystallizing the trespass requirement as central to Fourth Amendment jurisprudence.[43] This same reasoning was used to short circuit Fourth Amendment protections whenever the government used a confidential

---

use of [conversations intercepted by wiretapping] amounted to a violation of the Fourth . . . Amendment[].").

37. *Id.* at 464 ("The amendment does not forbid what was done here. . . . There was no entry of the houses or offices of the defendants.").

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

39. *Id.* ([T]he analogy fails. . . . [Sealed letters and packages are] plainly within the words of the amendment . . . . The [telephone conversations were] secured by the use of hearing and that only.").

40. *Id.* at 478 (Brandeis, J., dissenting).

41. Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1101 (2002), http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2/ ("[T]he Court frequently has invoked Brandeis's formulation of privacy as 'the right to be let alone.'") (citing Eisenstadt v. Baird, 405 U.S. 438 (1972), 454 n.10; Stanley v. Georgia, 394 U.S. 557, 564 (1969); Katz v. United States, 389 U.S. 347, 350 (1967)).

42. *See, e.g.*, *Katz*, 389 U.S. at 353 (rejecting *Olmstead*'s reliance on the trespass doctrine and holding that the Fourth Amendment proscribes the use of wiretaps that violate an individual's justifiable expectations of privacy); Silverman v. United States, 365 U.S. 505, 511 (1961) ("Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law.").

43. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding no Fourth Amendment violation because the device used to overhear defendants' conversation made no physical intrusion into defendant's office).

informant to solicit inculpatory information from suspects.[44] The Court reasoned that "[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak."[45] The Court placed great significance on the lack of physical trespass on a protected interest and deemed the deceit on the part of the informant to be of no consequence.[46]

B. Expectations of Privacy: A Pivot Towards a Normative Jurisprudence

In *Katz v United States*, the Court finally articulated what non-trespassory conduct the Fourth Amendment protected.[47] *Katz* involved a defendant convicted of "transmitting wagering information by telephone . . . in violation of a federal statute."[48] While presenting its case, the federal government offered recordings of phone conversations Katz made from a public telephone booth upon which the government affixed an "electronic listening and recording device."[49] Noting the Fourth Amendment protected "individual privacy against certain kinds of governmental intrusion," the Court held that the "[g]overnment's activities . . . violated the privacy upon which he justifiably relied while using the telephone booth . . . ."[50]

Central to the court's reasoning was the role telephone communications had come to play in society since *Olmstead* had been decided.[51] Ultimately, the Court established that "the Fourth Amendment protects people, not places. . . . [W]hat [someone] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[52] This assertion was not entirely novel as the Court had recognized "the right of a man to retreat into his own home and there be free from unreasonable

---

44. *See generally* Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952).

45. *Hoffa*, 385 U.S. at 303 (quoting *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting)).

46. *See Hoffa*, 385 U.S. at 302 (noting that "no interest legitimately protected by the Fourth Amendment" was implicated because the informant was invited into the room).

47. 389 U.S. 347. This is important to the cell phone context because trespass to chattel requires intentional physical contact with the chattel, which is absent in CSLI cases. RESTATEMENT (SECOND) OF TORTS § 217 cmt. e (1965).

48. *Katz*, 389 U.S. at 348.

49. *Id.*

50. *Id.* at 350, 353.

51. *Id.* at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

52. *Id.* at 351.

governmental intrusion" more than five years before the *Katz* decision.[53]

The majority's opinion focused on the case before the Court and left open the extent to which the Constitution protected individual privacy.[54] In an oft-quoted passage, Justice Harlan framed the Court's decision as "a twofold requirement[:] first that a person [exhibit] an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[55] Barely a decade later, the Court formally adopted this approach as the proper inquiry into what conduct the Fourth Amendment protects.[56]

Katz is the first instance of the Court adopting a normative analysis focused on society's privacy expectations over the prevailing trespass theories largely based on property interests and tort law.[57] Perhaps more significantly, the Court also found that Katz's expectation of privacy was reasonable, emphasizing that he was "surely entitled to assume" that his calls would not be overheard.[58]

Most important to the CSLI context, the Court rooted its holding on "the vital role that the . . . telephone has come to play in private communication."[59] Knowledge of the possibility of

---

53. Silverman v. United States, 365 U.S. 505, 511 (1961).

54. *Katz*, 389 U.S. at 354–58 (focusing on whether the Government in the current case ran afoul of the Constitution, but failing to establish a bright-line rule).

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

56. In *Smith v. Maryland*, the Court stated:

> This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy,"—whether, in the words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable,'"—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.

442 U.S. 735, 740 (1979).

57. *See Katz*, 389 U.S. at 353, 360–62; Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 597 (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471517.

58. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (quoting the majority in describing the government's argument and agreeing with the statement). The importance of this holding rests on the public's growing knowledge of the government's increased use of warrantless wiretaps during the period leading up to *Katz*. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 28 (2007), https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review-stlr/online/freiwald-first-principles.pdf ("In the several years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts.").

59. *Katz*, 389 U.S. at 352.

communications interception is not the test for reasonableness.[60] A government bulletin on television that advised all future phone calls were subject to monitoring would easily overcome such a test.[61] And if that were the case, "constitutional rights [would be] at the mercy of the executive branch, an entity which the Fourth Amendment was specifically designed to constrain."[62] Thus, *Katz* teaches that an individual's expectation of privacy does not turn on the "fact-of-interceptibility" of his communications.[63] Instead, courts must conduct a normative analysis and determine whether users of communications systems are "entitled to assume" that their actions or communications will not be monitored.[64]

Katz's reasonable expectation of privacy protection caused waves in the legal community and wrapped large swaths of unprotected conduct within the cloak of the Fourth Amendment.[65] However, even the *Katz* court realized that some conduct, though alleged to be subject to a reasonable expectation of privacy, would fall outside of the Fourth Amendment when the totality of the circumstances showed that the individual did not, in fact, expect privacy.[66] Because of this, it was unclear whether the Fourth Amendment prohibited law enforcement from using confidential informants to record conversations.[67] The cases appeared to depend on the absence of a physical trespass, which *Katz* held was no longer the test for determining Fourth Amendment protections.[68] At the same time, the Court has explained that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it" which cut against the subjective expectation prong of *Katz*.[69]

In *United States v. White*, the Court confirmed its previous confidential informant holdings and stated that the Fourth

---

60. *See* Freiwald, *supra* note 58 at¶¶ 22–35.

61. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

62. Freiwald, *supra* note 58, at ¶ 31.

63. *But see In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 613–14 (5th Cir. 2013).

64. Freiwald, *supra* note 58, at ¶¶ 28–35; *see also* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (noting that the second prong of *Katz* essentially calls on judges to make a value judgment).

65. Solove, *supra* note 41, at 1146 ("The *Olmstead* Court had clung to the outmoded view that the privacy protected by the Fourth Amendment was merely freedom from physical incursions. . . . [T]he court swept away this view in *Katz v. United States*.").

66. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person *knowingly exposes to the public*, even in his own home or office, is not a subject of Fourth Amendment protection.") (emphasis added).

67. Tokson, *supra* note 57, at 598.

68. *Katz*, 389 U.S. at 353.

69. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966).

Amendment does not protect communication an individual makes to another person.[70] The Court reasoned that a suspect assumes the risk that whoever he is speaking with may turn around and recount their communications to the police.[71] Because of this, any expectation of privacy in those conversations would be unreasonable.[72] Therefore, the Fourth Amendment does not protect statements that you make to another.[73]

C. Modern Third-Party Doctrine

In *United States v. Miller*, the Court drew upon *White* when determining whether an individual had an expectation of privacy protected by the Fourth Amendment in records maintained by his bank.[74] The District Court convicted Miller of (among other crimes) conspiracy to defraud the United States of tax revenue relating to his illicit whiskey production and distribution enterprise.[75] During their investigation of the conspiracy, the government secured from Miller's bank images of "checks, deposit slips, two financial statements, and three monthly statements" pertaining to Miller's accounts.[76] Some of these documents were introduced at trial to show overt acts in furtherance of the conspiracy.[77]

Characterizing the documents as illegally seized, Miller sought to have the evidence suppressed.[78] The District Court denied Miller's motion, but the Court of Appeals reversed, reasoning that the government had circumvented the Fourth Amendment's protection of an individual's private papers from unreasonable searches and seizures when it compelled the bank to produce and allow inspection of documents concerning Miller's bank account.[79] The Supreme Court then reversed the circuit

---

70. 401 U.S. 745, 752 (1971).

71. *Id.*

72. *See id.* at 752–53. Accordingly, the Court held that the government may introduce tape recordings of those conversations into evidence, because there is no difference between the informant testifying about his conversations at trial and tape recording those conversations for use as evidence. *Id.*

73. *See id.* Importantly, *White* was rooted in law enforcement's reliance on earlier precedents upholding the use of informants. Tokson, *supra* note 57, at 598. However, the Court lifted the assumption-of-risk rationale directly from the prior informant cases, which only addressed oral statements made in person to a government agent. *See White*, 401 U.S. at 752. It follows that *White* only denied Fourth Amendment protection to verbal conversations. *See White*, 401 U.S. at 750–52; *Hoffa*, 385 U.S. at 302– 03.

74. 425 U.S. 435, 442 (1976) ("But in *Katz* the Court also stressed that '(w)hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'") (alterations in original).

75. *Id.* at 436.

76. *Id.* at 438.

77. *Id.*

78. *Id.*

79. *Id.* at 439.

court, finding "no intrusion into any area in which respondent had a protected Fourth Amendment interest . . . ."[80]

Drawing on the "knowingly exposes" language of *Katz* and assumption-of-risk rationale in *White*, the *Miller* Court determined the bank records to be free of Fourth Amendment protections because they contained only information Miller had voluntarily given to the bank.[81] Recognizing that the government viewed only copies of Miller's checks and deposit slips, the Court noted as well established:

> that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[82]

By strengthening the assumption-of-risk connection between the Fourth Amendment and the Third Party Doctrine, the Court made clear that Fourth Amendment protections would not extend even if the originals had been the documents in question.[83]

White and the earlier informant cases were premised on the reality that revealing information to another person through conversation with another person opens you up to the risk that they will repeat your words to the police, regardless of what privacy expectations you had for that conversation.[84] In each of those decisions, the Court limited its holding to the facts before it. Indeed, *White* merely reiterated that the informant cases had survived *Katz*, and did not purport to extend the rule in those cases beyond verbal conversations.[85] Despite the Supreme Court's efforts to cabin *White* to the types of conversations in that case, the *Miller* court construed the decision to reach beyond conversations, yet offered no explanation as to why a suspect's bank records are constitutionally indistinguishable from his conversations with another person.[86]

Miller presented a fairly straightforward application of the "knowingly exposes" language in *Katz* because there was a

---

80. *Id.* at 440.

81. *Id.* at 442 ("The checks are not confidential communications . . . [They] contain only information voluntarily conveyed to the banks.").

82. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

83. *Id.* at 442 ("Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate 'expectation of privacy' in their contents.").

84. *See, e.g.*, *Hoffa*, 385 U.S. at 303.

85. *White*, 401 U.S. at 749–54.

86. *See Miller*, 425 U.S. at 443.

transfer of physical information from an individual to a third party. Three years later, the Court considered the question of how this Third-Party Doctrine applies to transfers of electronic, rather than physical, information.[87] In *Smith v. Maryland*, the petitioner (Smith) was convicted of robbery after phone calls he made to the victim were traced back to his home.[88] During their investigation of the robbery, and without a warrant, the police had a pen register (a mechanical device that records the numbers dialed on a telephone) installed at the telephone company's headquarter so as to record all the phone numbers Smith dialed from his home phone.[89]

The trial court denied Smith's motion to suppress and admitted the pen register evidence.[90] The Maryland Court of Appeals affirmed the judgment, reasoning "that there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment [sic] is implicated by the use of a pen register installed at the central offices of the telephone company."[91]

The Supreme Court agreed with the Maryland Court of Appeals and affirmed.[92] According to the Court, an individual could not reasonably have an expectation of privacy because he must know the intricacies of the telephone system.[93] The Court went further and suggested that individuals were not only aware of telephone switchboard operation protocols, but also that telephone companies used pen registers regularly.[94] Because "[t]elephone users . . . typically know that they must convey numerical information to the phone company . . . and that the phone company does in fact record this information," the Court could not fathom an individual "harbor[ing] any general expectation that the numbers they dial will remain secret."[95]

Channeling Justice Harlan, the Court elaborated that, notwithstanding Smith's subjective expectation of privacy, an

---

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

88. *Id.* at 737–38.

89. *Id.* at 737.

90. *Id.* at 737. Smith argued that the use of the pen register violated his "legitimate expectation of privacy" that the numbers he dialed would remain private. *Id.* at 741.

91. *Id.* at 738 (quoting Smith v. State, 389 A. 2d 858, 867 (Md. 1979).

92. *Id.* at 742–43 (1979) ("Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone. This claim must be rejected.").

93. *Id.* at 742 ("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.")

94. *Id.* ("Pen registers are regularly employed . . . .")

95. *Id.* at 743.

expectation that the phone numbers an individual dialed would remain private "is not one that society is prepared to recognize as 'reasonable.'"[96] After relating *Miller*'s central holding, the Court reasoned that Smith had voluntarily conveyed the telephone numbers to a third party thereby waiving any reasonable expectation of privacy.[97] Without a reasonable expectation, either objective or recognized by society, "[t]he installation and use of a pen register, consequently, was not a 'search,' and no warrant was required."[98]

From *Miller* and *Smith*, the Third-Party Doctrine was born; the result of combining two lines of cases, neither of which denied Fourth Amendment protection, and applying to all information that a person voluntarily conveys to a third party so as to deprive a right to privacy. Of note is the lack of any normative analysis in the *Smith* and *Miller* decisions.[99] Predictably, the broad holdings of *Miller* and *Smith* have resulted in a great reduction of personal privacy, as courts increasingly characterize emerging technologies as communications voluntarily disseminated to third parties. While this Comment does not advocate abolishing the Third-Party Doctrine, the leaps in the Court's reasoning in *Smith* and *Miller*, paired with the reality of changing personal digital technologies, demonstrate that the doctrine should, at the very least, be re-examined if not rolled back significantly.

---

96. *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

97. *Id.* at 744 ("[P]etitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company . . . . In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."). Foreshadowing the tension in *United States v. Jones*, much of the *Smith* and *Miller* third-party analysis borrows heavily from the assumption-of- risk doctrine in tort law. *Compare* United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.") *and Smith*, 442 U.S. at 744 ("[P]etitioner assumed the risk that the company would reveal to police the numbers he dialed.") *with* RESTATEMENT (SECOND) OF TORTS § 496A (1965) ("A plaintiff who voluntarily assumes a risk of harm . . . cannot recover for such harm.").

98. Smith, 442 U.S. at 743–745. The Court relied heavily on its recent decision in *Miller*, *White*, and *Couch v. United States*. *Id.* at 744. *Couch* denied Fourth Amendment protections to any person who gives tax records to his accountant to prepare a tax return because he knows the accountant will have to turn over the information to the government and, therefore, cannot have a reasonable expectation of privacy. Couch v. United States, 409 U.S. 322, 335–36 (1973). The analogy is inapt because even if Smith did not expect the numbers he dialed to remain private, he certainly did not have actual knowledge that the government would receive the numbers. *Smith*, 442 U.S. at 743–745.

99. This oversight has led to disagreement on the court in recent years. *Compare* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) *with id.*at 962 (Alito, J., concurring).

D. Third-Party Doctrine and CSLI

The Third-Party Doctrine plays a key role in Fourth Amendment jurisprudence because even the most genuine belief an individual may possess about the privacy of their conduct will fail if it is not an expectation "that society is prepared to recognize as 'reasonable.'"[100] Predictably, as CSLI has been litigated within the circuit courts, a split has emerged regarding whether individuals are "voluntarily conveying" their CSLI to service providers.[101] The question usually turns on whether the language of the contract releasing CSLI to service providers constitutes voluntary conveyance.

Most service contracts include clauses within their privacy policies informing consumers that service providers use individual's location information to route their calls and other services.[102] The policies explicitly state service providers also store this information.[103] Therefore, prosecutors have successfully argued that by agreeing to the terms of service, subscribers voluntarily consent to the disclosure of CSLI to service providers and, as a result, cannot reasonably expect privacy in that data.[104] Accordingly, the Fourth Amendment does not bar the government from compelling production of the subscriber's CSLI and introducing it as evidence against him or her in a criminal proceeding.[105] However, for courts who rely on *Smith* and *Miller*, that language obviates any reasonable expectation of privacy.[106]

The Fifth Circuit focused on the post-collection privacy interests when it held that cell phone users do not have a reasonable expectation of privacy in CSLI.[107] According to the court, since consumers are aware CSLI is emitted for service and

---

100. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also Smith*, 442 U.S. at 743.

101. *Compare In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("We understand that cell phone users may reasonably want their location information to remain private . . . . [But t]he Fourth Amendment . . . protects only reasonable *expectations* of privacy.") *and* United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014) ("[C]ell phone users voluntarily convey [CSLI] to their service providers . . . .") *with* United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015) ("Cell phone users have an objectively reasonable expectation of privacy in [CSLI].").

102. *In re Application of United States for Historical Cell Site Data*, 724 F.3d at 613 .

103. *Id.*

104. *See id.*; *see also In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3rd Cir. 2010).

105. *See In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317.

106. Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (relying, in part, on a notice published in a company's phone book stating that the company frequently helps authorities with investigations as reason to dismiss claim of a reasonable expectation of privacy).

107. *See In re Application of United States for Historical Cell Site Data*, 724 F.3d at 611–15.

voluntarily continue to use their cell phones, cell phone users do not have an expectation of privacy in CSLI.[108]

In *In re Application of United States for Historical Cell Site Data*,[109] the Fifth Circuit considered the government's appeal of a denial of a request for historical cell site data on the ground that the compelled warrantless disclosure of CSLI would violate the Fourth Amendment.[110] Reminiscent of *Miller*, the court focused on the fact that CSLI is essentially a business record of cell providers.[111] The CSLI records are equivalent to "the providers' own records of transactions to which it is a party," and providers gather this data in accordance with the privacy policy within the service contract.[112]

The Fifth Circuit proceeded to dismantle arguments that cell phone users do not voluntarily convey CSLI to cell providers and therefore have a protected privacy interest in CSLI.[113] The court relied on consumer's voluntary continued use of their devices despite knowledge of CSLI being conveyed to service providers during use.[114] In doing so, the court imputed all users with the knowledge that cell phones must send signals to cell towers in order to connect to a call.[115] Acknowledging that perhaps not all users are aware of the technological workings of cell phones, the court reasoned consumers are aware of CSLI emissions because service agreements and privacy policies are explicit about how providers use CSLI to route phone calls and subsequently store the data.[116] Following this train of thought, the court held that cell phone users "understand that their service providers record their location information when they use their phones . . . ."[117]

The Fifth Circuit did recognize "that cell phone users may reasonably want their location information to remain private . . . ."[118] Regardless of this desire, the court was convinced that citizens do not "expect" privacy.[119] The Fifth Circuit presumed

---

108. *See id.* at 612–13.

109. *Id.*

110. *Id.* at 602 (citing In re Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010)).

111. *Id.* at 611–12.

112. *Id.* at 612. The court found significance in the fact that cell providers gather CSLI but not transcripts of users' calls. *Id.*

113. *Id.* at 612–13.

114. *Id.*

115. *Id.*

116. *Id.* at 613.

117. *Id.* To reach this conclusion, the court referenced *Smith*'s reasoning that consumers do not have a protected interest in telephone numbers dialed because telephone companies record the numbers dialed. *Id.* at 612.

118. *Id.* at 615.

119. *See id.*

that the average cell phone user has an intricate working knowledge of how cell phones work. Not a single study documenting public understanding was cited, but rather the court assumed that each customer reads all the fine print in their service agreements.[120] The Fifth Circuit essentially ignored the second prong of *Katz* and focused on the existence of CSLI emissions, rather than whether consumers have any expectation of privacy analogous to stepping into a phone booth to make a call.[121]

IV. THE MODERN COURT'S FOURTH AMENDMENT PERSPECTIVE

Despite language to the contrary, the Court has recently held that *Katz*'s formulation is not the entirety of modern Fourth Amendment jurisprudence despite the opinion's language to the contrary.[122] Although the Court has been reluctant to decide whether CSLI is protected by the Fourth Amendment, the discussion presented by the three opinions in *United States v. Jones* shows that the current Court is serious about considering constitutional questions as they relate to societal expectations.[123] Part IV.A considers what the varying opinions in *Jones* reveal about the current justices' Fourth Amendment views. Part IV.B surveys recent circuit court opinions decided since *Jones* regarding CSLI.

A. Third Party Doctrine and Modern Technologies in the Jones Court

In *United States v. Jones*, the Court considered whether using Global-Positioning System (GPS) technology to track an individual's whereabouts by attaching it to his vehicle violated the Fourth Amendment.[124] Though *Jones* is mostly of interest because of Justices Sotomayor's and Alito's concurring opinions, all three opinions provide a full-throated challenge to the wisdom of continuing the Third-Party Doctrine and reveal a Court that is willing to reassess the Fourth Amendment in light of new technologies.[125]

---

120. *See id.* at 613.

121. *See id.* at 613–14. Telling is the dissent's admission that there is doubt as to whether consumers have a reasonable expectation of privacy in CSLI. *See id.* at 623–24 (Dennis, J., dissenting) (citing Justices Sotomayor's and Alito's concurring opinions in United States v. Jones, 132 S. Ct. 945, 955–57, 963(2012)).

122. *Compare Jones*, 132 S. Ct. at 950 ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass . . . . *Katz* did not repudiate that understanding.") *with* Katz v. United States, 389 U.S. 347, 353 (1967) ("We conclude . . . that the 'trespass' doctrine . . . can no longer be regarded as controlling.").

123. *Jones*, 132 S. Ct. 945.

124. *Id.* at 948.

125. *See id.* at 954–57 (Sotomayor, J., concurring), 957-64 (Alito, J., concurring).

Law enforcement officers used information obtained from a GPS device to secure the conviction of Jones on multiple drug-related offenses.[126] The Supreme Court affirmed the D.C. Circuit's decision, overturning the conviction because the warrant for the GPS required the device be placed within ten days of issuance while in the District of Columbia, but the device was attached to the vehicle on the eleventh day in Maryland.[127] Writing for the majority, Justice Scalia concluded that the precedents since *Katz* made clear that the "reasonable-expectation-of-privacy test [was] *added to*, not *substituted for*, the common-law trespassory test."[128]

Befuddled by the majority's opinion, Justice Alito's concurrence analyzed the case solely based on the *Katz*'s reasonable-expectation-of-privacy test.[129] For Justice Alito, the majority's opinion failed to fully consider the fundamental issue of the case.[130] Instead of focusing on "18th-century tort law," Justice Alito believed the case presented an opportunity to bring the Fourth Amendment into the twenty-first century and consider whether "surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked" constituted a search and seizure under the Fourth Amendment.[131]

In a separate concurrence, Justice Sotomayor agreed with Justice Alito that longer-term GPS monitoring violates reasonable expectations of privacy.[132] Justice Sotomayor raised concerns about how "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[133] Beyond precision, Justice Sotomayor reasoned that GPS's relative low cost compared to traditional tracking methods, coupled with its surreptitious nature, allows GPS to "evade[] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[134] Because of the effects GPS monitoring poses to the American system of government, Justice Sotomayor argued that "the Government's unrestrained power to assemble data that

126. *Id.* at 948–49.

127. *See id.*

128. *Id.* at 952.

129. *Id.* at 957–58 (Alito, J. concurring).

130. *Id.* at 961 ("[T]he Court's reasoning largely disregards what is really important (the *use* of a GPS for purpose of long-term tracking).").

131. *Id.* at 957, 962 The tension between tort law and Fourth Amendment is no new conflict. Silverman v. United States, 365 U.S. 505, 511 (1961) ("Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law.").

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

133. *Id.*

134. *Id.* at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[135]

Justice Sotomayor then declaimed the Third-Party Doctrine itself as "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."[136] Her problem with the doctrine is that it "treat[s] secrecy as a prerequisite for privacy," forcing individuals to forgo all constitutional protection if they disclose information to a single entity for a limited purpose.[137] Therefore, Justice Sotomayor "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."[138]

Instead of confronting the concerns of Justices Alito and Sotomayor, the majority opinion refused to consider the *Katz* paradigm, believing that the trespass theory disposed of the case.[139] While *Jones* may not have required the Court to decide them, new petitions have begun presenting the issue as it pertains to CSLI.[140] This is unsurprising because *Jones* exposed a Court that would not automatically apply the Third-Party Doctrine to CSLI or similar technologies. Curious, though, is that the Court declined to consider the question as recently as 2015.[141]

B. Jones's Circuit Court Impact

Addressing the issue head-on, the Third, Fourth, and Eleventh Circuits have each declined to apply the Third-Party Doctrine to CSLI.[142] All three circuits rejected the government's

---

135. *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

136. *Id.* at 957.

137. *Id.*

138. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy 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 business purpose need not assume that this information will be released to other persons for other purposes")).

139. *Id.* at 950 (majority opinion) ("But we need not address the Government's [argument about reasonable expectations of privacy], because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

140. *See, e.g.*, United States v. Davis, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (asking whether the Fourth Amendment permits the warrantless seizure of historical cell phone records revealing the location and movements of a cell phone user).

141. *Id.*

142. *See* United States v. Graham, 796 F.3d 332, 352–61 (4th Cir. 2015); United States v. Davis, 754 F.3d 1205, 1216-17 (11th Cir. 2014); *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317–19 (3d Cir. 2010).

Third-Party Doctrine argument, focusing on the empirical finding that cell phone users are generally not aware that placing a call emits CSLI to the cell provider which the provider then stores.[143] As the Third Circuit noted, cell phones emit CSLI even if the user has not voluntarily exposed anything—as when a call is received or the phone is merely turned on.[144] Borrowing from *Smith*, all three circuits held that the only information cell phone users knowingly expose is the number they dial when they place a call. Therefore, cell phone users are entitled to assume that their CSLI will remain private.[145] Because the Third Circuit issued their opinion before *Jones*, this Comment will focus on the decisions out of the Fourth and Eleventh circuits.

The Eleventh Circuit in *United States v. Davis*[146] held that cell phone users have a reasonable expectation of privacy in CSLI.[147] First, the court held that "even one point of cell site location data can be within a reasonable expectation of privacy," because CSLI "is private in nature . . . ."[148] The court stressed that a person may assume that "even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, . . . the visit is private if it was not conducted in a public way."[149] In this respect, CSLI is distinct from an automobile's GPS data. It is only the aggregation of the GPS data that violates a person's expectation of privacy in their otherwise public movements; the concern in the CSLI contexts arises from individual data points potentially revealing personal location.[150] By contrast, a "cell phone . . . can accompany its owner

---

143. *Graham*, 796 F.3d at 356; *Davis*, 754 F.3d at 1217; *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317.

144. *See In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317–18.

145. *See Davis*, 754 F.3d at 1216–17; *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317 (3d Cir. 2010); *cf. Graham*, 796 F.3d at 356 (finding *Miller* and *Smith* insufficiently analogous because a lack voluntary conveyance of CSLI).

146. 754 F.3d 1205 (11th Cir. 2014), *vacated in part en banc*, 785 F.3d 498 (11th Cir. 2015). Because an en banc panel of the Eleventh Circuit reheard *Davis*, the opinion of the three-judge panel has been vacated in part. Regardless, the opinion of the three-judge panel is still important for its reasoning regarding the applicability of the Third-Party Doctrine and a demonstration of the developing circuit split.

147. *Id.* at 1217 ("[W]e hold that cell site location information is within the subscriber's reasonable expectation of privacy.").

148. *Id.* at 1216.

149. *Id.*

150. *Id.* ("GPS location information on an automobile would be protected only in the case of aggregated data . . . ."). GPS tracking only reveals the vehicle's movements, which will mostly be limited to public roads and parking lots. By contrast, CSLI effectively reveals the subscriber's movements, as most subscribers carry their cell phone on their person throughout the day. Therefore GPS tracking of a vehicle is much less useful as an indicator of the places the driver went during the surveillance period. CSLI is more akin to placing a tracking device in the subscriber's pocket, as it creates a much more

anywhere."[151] Thus, the exposure of even one data point "can convert what would otherwise be a private event into a public one."[152]

The court then addressed the government's argument that Davis forfeited any expectation of privacy in his CSLI because he "surrendered that expectation by exposing his cell site location to his service provider when he placed the call."[153] The court disagreed with the government, holding that "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."[154] The court further held that the only information a cell phone user knowingly conveys when placing a call is the dialed number because "there is no indication to the user that making that call will also locate the caller."[155] The court concluded that Davis's CSLI transmissions to his cell provider were not voluntary disclosures and he had not forfeited his reasonable expectation of privacy.[156]

In *United States v. Graham*, the Fourth Circuit followed the Eleventh in holding that consumers have a reasonable expectation of privacy in their CSLI.[157] The Fourth Circuit found that, unlike the telephone user in *Smith* who knowingly conveyed the number dialed, the cell phone user in *Graham* did not voluntarily share her location in any meaningful way.[158] Similar to Justice Sotomayor's concurring opinion in *Jones*, the Fourth Circuit was adamant that neither *Smith* nor *Miller* categorically exclude all information within third-party records.[159] The court read the

---

comprehensive picture of all the places he or she has been. *See id.*; *see also* Freiwald, *supra* note 3, at 702.

151. *Davis*, 754 F.3d at 1216.

152. *Id.*

153. *Id.*

154. *Id.* at 1216–17 (emphasis omitted) (quoting *In re* Application of United States 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)).

155. *Id.* at 1217 (quoting *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317). The prosecutor even argued that Davis "probably had no idea that by bringing [his] cell phone[] with [him] to these robberies, [he was] allowing [his] [cell service provider] . . . to follow [his] movements on the days and at the times of the robberies. . . ." *Id.* at 1217 (sixth and last alterations in original).

156. *Id.*

157. 796 F.3d 332, 345 (4th Cir. 2015), *aff'd*, 824 F.3d 421 (4th Cir. 2016). Much like *Davis*, an en banc panel of the Fourth Circuit reheard *Graham* and affirmed the three-judge panel's opinion. The opinion of the three-judge panel still provides great insight into how courts may apply the Third-Party Doctrine in light of recent Supreme Court decisions and a demonstration of the developing circuit split.

158. *Graham*, 796 F.3d at 352–55 ("A user is not required to *actively* submit any location-identifying information when making a call or sending a message.") (emphasis added).

159. *Id.* at 354.

Third-Party Doctrine only to exclude information that individuals voluntarily convey to third parties because, in doing so, individuals assume the risk upon which is the foundation of the Third-Party Doctrine.[160]

The court also found that the fact the company's privacy policies mentioned this collection did not suggest a different conclusion because most users are not familiar with or otherwise understand their provider's policies.[161] Nor was the Fourth Circuit persuaded that individuals choose to convey their location information when they activate their cell phones and carry them around on their person.[162] Instead, the court recognized the ubiquitous nature of cell phone use in modern society, which led to the court recognizing society retained a reasonable expectation of privacy in their CSLI.[163]

Both *Davis* and *Graham* represent the circuit courts reimagining the Third-Party Doctrine in light of the *Lopez* decision and changing digital technologies. As the Supreme Court continues to signal a shift in thinking toward the Fourth Amendment and digital technologies, these courts will be the test kitchens for what protection society expects within the digital age.[164]

V. CONCLUSION

The *Katz's* Fourth Amendment analysis should protect CSLI and other third-party data from warrantless government searches and seizures. *Davis* and *Graham* represent the most logical approaches to applying the *Katz* test to CSLI, as it not only grapples with the mechanics of how cell phone users generate CSLI, but also gives sufficient weight to subscribers' privacy interests. Many state high courts have already developed excellent

---

160. *Id.*

161. *Id.* at 345. In so holding, the court relied on several studies which support the proposition that many consumers "do not read or understand their providers' privacy policies." *Id.* (citing F.T.C., *MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY* 10 (Feb. 2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

162. *Id.* at 355.

163. *Id.* at 355–57. The Fourth Circuit was explicit in rejecting any imputation of knowledge about how cell phone technology operates to ordinary citizens because that knowledge is wholly beside the point for Fourth Amendment analysis. *Id.*

164. *See* Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 DUKE J. CONST. L. & PUB. POL'Y 83, 109 (2015). http://scholarship.law.duke.edu/djclpp/vol10/iss1/4/ (noting the impact recent *Riley v. California* may have on Fourth Amendment jurisprudence in regards to various aspects of digital technology).

reasoning for allowing Fourth Amendment protection to CSLI.[165] The Fifth Circuit, by contrast, gave short shrift to the normative analysis required by *Katz*. Instead of considering what, if any, expectations of privacy society places on CSLI, the court equated the automatic emission of CSLI to voluntarily conveying location data to a third party.[166] Despite the recent denial of certiorari in *United States v. Davis*, the split between circuits about whether warrantless government requisition and use of CSLI constitutes an unreasonable search and seizure seems destined for Supreme Court review.[167]

Matthew A. Harper

165. *See generally* State v. Earls, 70 A.3d 630 (N.J. 2013); Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014); Tracey v. State, 152 So. 3d 504 (Fla. 2014).

166. *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 612–15 (5th Cir. 2013). *See supra* notes 107-121 and accompanying text (discussing the Fifth Circuit's assumptions regarding consumers and cellular service contracts).

167. *Compare Graham*, 796 F.3d at 343 *and* United States v. Davis, 754 F.3d 1205, 1215–17 (11th Cir. 2014), *cert. denied,* 136 S. Ct. 479 (2015) *with In re* Application of United States for Historical Cell Site Data, 724 F.3d at 612–15 (5th Cir. 2013).