The University of the Pacific Law Review

Volume 48 | Issue 2 Article 18

1-1-2017

The "Big Brother" Effect: The Implications of the Unanswered Question in United States v. Jones

Heather Phillips
The University of Pacific, McGeorge School of Law

The "Big Brother" Effect: The Implications of the Unanswered Question in *United States v. Jones*

*Heather Phillips**

TABLE OF CONTENTS

I. INTRODUCTION

In a society dominated by technology, a cell phone is no longer a luxury, but a necessity. 90% of American adults own a cell phone, and 64% of American adults own a smartphone.[1] Three-quarters of Americans owning a smart phone

* J.D. Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2017; B.A., Legal Studies and History, University of California, Santa Cruz, 2013. I would like to thank my advisor, Professor Michael Vitiello, for all the time and energy he dedicated to helping me write this comment. I would also like to thank all of the editors whose sleepless nights made this Comment possible. Finally, I want to thank my mom and dad. Without them, I wouldn't be where I am today.

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

claim to be within five feet of it at all times.[2] Twelve percent of users even claim to use their smartphone in the shower.[3] These statistics support the following assertion made in *Riley*:

> [M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.[4]

Always keeping a cell phone in close proximity, one inevitably carries the device to and from private places. However, many people are unaware that carrying this device may allow the government to track their movements down to the minute.[5] Imagining a world where the government has access to a person's location every time a cell phone is in close proximity is frightening. Imagining a world where not only does the government have access to this information, but can obtain it and use it without probable cause and without a warrant is even more daunting. Due to loopholes in Fourth Amendment case law, this is not something we have to imagine.[6] This may be the world we live in.[7]

In *Jones*, law enforcement officers placed a tracking device below Jones' vehicle and tracked his movements for 28 days.[8] The Court relied on the physical trespass—the placing of the device underneath the vehicle—to conclude a search occurred within the meaning of the Fourth Amendment.[9] However, the Court's approach left unanswered whether tracking Jones' movements on public roadways without a physical trespass would constitute a search.[10] Circuit courts are split on how to resolve it.[11]

Circuit court case law reveals tension between the right to privacy and rapidly evolving surveillance techniques using advanced technology.[12] Because new technology available today is even more invasive than the technology used in cases like *Jones*, the Supreme Court needs to address the unanswered question in *Jones* to preserve Fourth Amendment protections in this era of emerging technology. Properly answering this question requires acknowledging the place cell phones have in a modern society along with a cell phone's ability to reveal intimate details about an individual's private life through his or her location at

2. *Id.*
3. *Id.*
4. *Id.* at 2484.
5. *Id.* at 2490.
6. *Id.* at 2494.
7. *Id.*
8. United States v. Jones, 132 S. Ct. 945, 946 (2012).
9. *Id.*at 949.
10. *Id.* at 946.
11. *See Infra* Part III (explaining the circuit split caused by the holding in *United States v. Jones*).
12. *Id.*

essentially any given moment.[13] A modern cell phone contains a "digital record" of almost every aspect of the owner's life "from the mundane to the intimate."[14] Due to the nature of modern cell phones and the frequency in which they travel to and from potentially intimate, private places with individuals, law enforcement use of noninvasive, cell site simulators to discover location information constitutes a search within the meaning of the Fourth Amendment, thereby requiring probable cause and a warrant.[15]

This Comment discusses the Fourth Amendment case law involving police use of surveillance technology leading up to *United States v. Jones.*[16] It then explains the *Jones* decision and the question the Supreme Court left unanswered: When does police use of surveillance technology, absent a physical trespass, constitute a search within the meaning of the Fourth Amendment?[17] This Comment then addresses the prominent circuit court split regarding whether one voluntarily discloses his or her location information to a third party through the use and possession of an operable cell phone, resulting from the unanswered question in *Jones*.[18]

After illustrating the circuit split, this Comment explains why the Supreme Court should adopt the Fourth Circuit's approach that one does not voluntarily disclose location information to a third party simply by using his or her cell phone.[19] Supporting the Fourth Circuit's approach, this Comment then describes the invasive nature of cell site simulators law enforcement currently use for surveillance.[20] In short, a cell site simulator essentially "tricks" cell phones in the surrounding geographical area to send the simulator signals revealing the location of the cell phone.[21] This Comment then highlights the flaws in other circuit's approaches.[22]

Highlighting the highly invasive nature of these devices and the private information they can potentially reveal,[23] it's unsurprising that use of these

13. *Jones*, 132 S. Ct. at 956–57.

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

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

16. *See infra* Part II.B (describing the Fourth Amendment case law preceding *United States v. Jones*).

17. *See infra* Part II.C (explaining the holding in *United States v. Jones* and how a physical trespass allowed the court to leave a question unanswered).

18. *See infra* Part III (illustrating the circuit split caused by the holding in United States v. Jones).

19. *See infra* Part IV (elaborating on the numerous reasons the Fourth Circuit's approach is the most in tune with modern realities and Fourth Amendment principles).

20. *See infra* Part IV.A (explaining how certain cell site simulators work without requiring a physical trespass).

21. *See infra* Part IV.A (explaining how cell site simulators operate as surveillance devices).

22. *See infra* Part IV.B (elaborating on how the Fifth and Sixth Circuit's holding that one voluntarily discloses location information to a third party by simply using his or her cell phone disregards the realities of modern cell phones and will erode privacy rights as technology advances).

23. *See infra* Part IV.C (comparing the nature of the devices employed in the Fourth Amendment cases preceding *Jones* and in *Jones* to new technology).

devices creates tension between law enforcement and citizens.[24] If the Court does not address the unanswered question, police will continue to utilize these devices freely and outside the realm of the protections guaranteed by the Fourth Amendment. Citizen outrage and curiosity as to the nature of these devices will grow.[25] Permitting police to exploit this hole in Fourth Amendment jurisprudence by engaging in advanced surveillance technology is a gross deviation from what the Framers of the United States Constitution intended and takes society back to the dark days of general warrants.[26]

II. THE FOURTH AMENDMENT FRAMEWORK

Section A discusses the critical facts in *Jones*, including law enforcement's use of a global positioning system (GPS) device to track Jones' movements over an extended period.[27] Section B discusses the Supreme Court precedent that bound *Jones*.[28] The cases discussed in Section B all involve Fourth Amendment challenges to the use of warrantless police surveillance technology without probable cause.[29] Section C elaborates on the holding in *Jones* and explains how the majority relied on the physical placing of the GPS device on Jones' car to find that a search occurred within the meaning of the Fourth Amendment.[30] Section D highlights the concurring opinions that foresaw the problems the majority's reliance would cause future courts when presented with similar facts absent the physical trespass.[31]

A. The Facts of Jones

In 2012, Antoine Jones was suspected of trafficking in narcotics and subsequently became a target of the FBI and local police department.[32] The police department installed a GPS device underneath Jones' vehicle and tracked

24. *See infra* Part IV.D (detailing a pending lawsuit against the Sacramento County Police Department as a result of its use of cell site simulators as part of its investigatory practices).

25. *See infra* Part IV.D (elaborating on the notion that government agents actively conceal information regarding these devices, and how citizens are discovering details about the devices' intrusive nature and detrimental impact on privacy rights).

26. William Cuddihy, *Warrantless House-to-House Searches and Fourth Amendment Originalism: A Reply to Professor Davies*, 44 TEX. TECH L. REV. 997, 998 (2012).

27. *See infra* Part II.A (providing the relevant facts of *United States v. Jones*).

28. *See infra* Part II.B (elaborating on the existing case law when *United States v. Jones* was decided).

29. *See infra* Part II.B (elaborating on the existing case law involving warrantless police use of technology when United States v. Jones was decided).

30. *See infra* Part II.C (explaining how the majority in *United States v. Jones* based their holding on pre-*Katz* law governing the Fourth Amendment).

31. *See infra* Part II.D (explaining how the majority in *United States v. Jones* based their holding on pre-*Katz* law governing the Fourth Amendment, while the concurring opinions saw the issues with this approach in the modern era).

32. United States v. Jones, 132 S. Ct. 945, 948 (2012).

the vehicle's movements for the next 28 days.[33] The location information obtained from the GPS device placed Jones at an alleged co-conspirator's house with over $850,000 in cash and a vast amount of narcotics inside.[34] The jury convicted Jones and the court sentenced Jones to life in prison.[35]

However, on appeal the United States Court of Appeals for the District of Columbia Circuit reversed his conviction.[36] The court employed the *Katz* analysis and held that when the police tracked the vehicle for 28 days, a search took place within the meaning of the Fourth Amendment.[37] Therefore, the police action required probable cause and a warrant.[38] The court reached this conclusion because "a reasonable individual would not expect that the sum of her movements over a month would be observed by a stranger in public, and this information could reveal an intimate picture of her life not disclosed by any one of her movements viewed individually."[39]

The Supreme Court granted certiorari and held the attachment of the GPS device to Jones' vehicle and subsequent use of that device to track the vehicle's movements on public roadways constituted a search within the meaning of the Fourth Amendment.[40] However, the court did not determine whether the same police conduct would constitute a search absent the physical trespass, which led to confusion amongst an already perplexing framework.[41]

B. The Road to United States v. Jones

The Fourth Amendment provides, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause. . . ."[42] The case law governing the application of the Fourth Amendment was complex prior to *Jones*.[43]

Common law trespass initially governed the Fourth Amendment cases using a property-based approach.[44] However, after 1967 courts began using the test laid

33. *Id.*

34. *Id.*

35. *Id.* at 949.

36. *Id.*

37. *Id.*

38. *Id.*

39. United States v. Graham, 796 F.3d 332, 347 (4th Cir. 2015).

40. *Jones*, 132 S. Ct. at 954, 964.

41. *Id.* at 954 (the court also left open whether law enforcement must obtain a warrant if the same police conduct, absent a physical trespass, constitutes a search).

42. U.S. CONST. amend. IV.

43. *See infra* Part II.B (explaining the complicated case law existing when *United States v. Jones* was decided).

44. *Jones*, 132 S. Ct. 950.

out in Justice Harlan's concurrence in *Katz v. United States*.[45] Justice Harlan explained that a search, within the meaning of the Fourth Amendment, occurs when police conduct violates a person's reasonable expectation of privacy.[46] The *Katz* test arguably broadens the scope of protections under the Fourth Amendment, relying on the notion that the Fourth Amendment protects people rather than places.[47] The test no longer relies on whether law enforcement commits a physical trespass on a constitutionally protected area to decide whether the government action triggers the Fourth Amendment protections.[48]

Following *Katz*, the Supreme Court decided a number of cases applying the *Katz* framework to situations involving law enforcement use of surveillance technology.[49] First, in *Smith v. Maryland*, a telephone company installed a pen register at the government's request and used it to discover phone numbers Smith dialed from inside his house.[50] The Court held this action was not a search within the meaning of the Fourth Amendment.[51] The Court reasoned that as a subscriber one realizes, or should realize, phone companies obtain the numbers dialed for reasons such as billing and keeping business records.[52] Further, pen registers reveal only the phone numbers dialed and not content of communications.[53]

As a result, the Court concluded Smith assumed the risk the phone company would reveal the numbers he dialed to the police.[54] Using the third party doctrine,[55] the Court held Smith did not have a reasonable expectation of privacy over the numbers he dialed because he voluntarily conveyed that information to his service provider when he dialed the numbers on his phone.[56]

In *United States v. Knotts*, the government installed a radio transmitter in a container of chloroform, prior to Knotts purchasing the container, and subsequently tracked the movements of the container on public roads while the container was in Knotts' possession.[57] The Court in *Knotts* used the *Katz* test to hold the government action did not constitute a search within the meaning of the

45. *Id.*

46. *See id.* at 954 (explaining that one must have a subjective expectation of privacy that society is ready to recognize as reasonable to satisfy the test).

47. Katz v. United States, 389 U.S. 347, 351 (1967).

48. *Id.* at 352.

49. *See infra* Part II.B (describing the case law that used the *Katz* test and subsequently shaped the Fourth Amendment Jurisprudence).

50. Smith v. Maryland, 442 U.S. 735, 737 (1979).

51. *Id.* at 742.

52. *Id.* at 741.

53. *Id.*

54. *Id.* at 744.

55. *See id.* (explaining the third party doctrine as the notion that one does not have a reasonable expectation of privacy over information he or she voluntarily discloses to third parties).

56. *Id.* at 744.

57. United States v. Knotts, 460 U.S. 276, 277 (1983) (The fact that the beeper was placed in the container prior to Knotts purchasing it is important because since he did not own the container when the beeper was installed, the police did not commit a physical trespass, forcing the court to conduct the *Katz* analysis).

Fourth Amendment because an individual has no reasonable expectation of privacy on public highways where any member of the public can see his or her movements.[58]

One year after *Knotts*, the Supreme Court decided *United States v. Karo*.[59] In *Karo*, the government again placed a beeper inside of a container Karo purchased and tracked the container's movements.[60] However, in *Karo* the Court held that a search occurred because unlike *Knotts*, where the monitoring took place entirely in public, the monitoring in *Karo* continued inside the home.[61]

Following *Knotts* and *Karo* was *Kyllo v. United States*.[62] In *Kyllo*, the Court held the police use of a thermal-imaging device from a public street to discover heat emanating off petitioner's home from a room used to grow marijuana, was a search within the meaning of the Fourth Amendment.[63]

Using the *Katz* formula and existing framework developed in the aforementioned cases, the government in *Jones* argued that since Jones had no reasonable expectation of privacy underneath his vehicle and on public roadways, no search occurred.[64] Since these areas were visible to the public, the government contended that Jones voluntarily relinquished any reasonable expectation of privacy he may have had.[65]

C. The Question Left Unanswered in United States v. Jones

Although the Supreme Court in *Jones* was working under this framework, it did not apply Harlan's concurrence in *Katz* to determine whether a search occurred.[66] By failing to do so, *Jones* further complicates the framework.[67] Writing for the majority, Justice Scalia explained that Jones' Fourth Amendment rights did not fall within the *Katz* formulation because the government committed a physical trespass when they placed the GPS device beneath Jones' vehicle.[68] Because of this, the Court employed the pre-*Katz* physical trespass test.[69] As a

58. *Knotts*, 460 U.S. at 285.

59. *See* United States v. Karo, 486 U.S. 703, 703 (1984) (holding the warrantless monitoring of a beeper in a private residence, a location not open to visual surveillance from a public space, violates the Fourth Amendment).

60. *Id.* at 708.

61. *Id.*at 714.

62. *See* Kyllo v. United States, 533 U.S. 27 (2001) (holding when a device, not in general public use, is subsequently used to discover details unknown to the public, without a physical intrusion, the surveillance is a search).

63. *Id.* at 40.

64. United States v. Jones, 132 S. Ct. 945, 950 (2012).

65. *Id.*

66. *Id.*

67. Ebony Morris, *Always Eyes Watching You: United States v. Jones and Congress's Attempts to Stop Warrantless Government Surveillance*, 40 S.U. L. REV. 489, 490 (2013).

68. *Id*.

69. *Id.* at 953.

result, the Court held that the government's action of placing the GPS device underneath the vehicle constituted a search within the meaning of the Fourth Amendment.[70]

Justice Scalia explained that *Katz* simply supplemented the previous property rights and the common law trespass regime governing the Fourth Amendment.[71] The court reasoned that a search undoubtedly occurs when the government gains information by physically intruding on a constitutionally protected area.[72] However, this presented a vexing problem for the concurring opinions.[73] The concurring opinions anticipated facing future situations where there is no physical intrusion into a constitutionally protected area, but rather, a situation involving only the "transmission of electronic signals" in light of rapidly growing technological advances.[74] The majority in *Jones* explained that such cases will still be analyzed under *Katz*.[75] However, since *Knotts* essentially permits a certain amount of warrantless government surveillance, at what point does this police conduct become a search requiring a warrant based on probable cause?[76] The majority opinion did not provide any guidance on how to tackle that issue, but the concurring opinions did.[77]

D. The Forward-Looking Concurring Opinions

Although concurring in the judgment, Justice Sotomayor provided the critical fifth vote for the *Jones* majority. She agreed with the majority's use of the pre-*Katz* physical trespass test, but explained how such a physical invasion constitutes a constitutional minimum.[78] She recognized that because of advances in technology, many types of police surveillance techniques do not require a physical trespass to be employed.[79] In future cases, where the government does not commit a physical trespass, Justice Sotomayor explained that she would take the attributes of GPS devices into account when considering whether there is a reasonable expectation of privacy "in the sum of one's public movements."[80]

An attribute of a GPS device she would take into consideration is the nature of the information the device can disclose to the government.[81] Justice

70. *Id.* at 949.

71. *Id.* at 952.

72. *Id.* at 955.

73. *See Infra* Part II.D (elaborating on the concurring opinions in *Jones*).

74. United States v. Jones, 132 S. Ct. 945, 955 (2012).

75. *Id.* at 953.

76. United States v. Knotts, 460 U.S. 276, 276 (1983).

77. *See infra* Part II.D (elaborating on the concurring Justices' attempt to tackle the issue the majority opinion ignored).

78. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

79. *Id.*at 955.

80. *Id.* at 956.

81. *Id.*

Sotomayor explained that GPS devices track one's public movements, which may reveal extremely private information such as, a trip to the plastic surgeon, a trip to the abortion clinic, a trip to the AID's treatment center, etc.[82] She believes it is foolish to think one does not have a reasonable expectation of privacy at these various locations.[83] Further, Justice Sotomayor expressed concern about the third-party doctrine.[84] In her view, this doctrine has no place in the digital age, where most individuals disclose a vast amount of information about themselves to third parties through routine and everyday tasks.[85]

Justice Alito, also concurring in the judgment, agreed with the majority's holding, that the police conduct constituted a search, but disagreed with the majority's approach.[86] He criticized the majority for using "18th-century tort law" to decide a case involving modern technology and surveillance techniques.[87] Alito argued that the current Fourth Amendment case law did not support the majority's "superficial" analysis.[88] Instead, he analyzed the issue under the *Katz* test.[89] His argument focused on the flaws of depending on a physical trespass because, in today's world, advanced technology and science can create much more intrusive devices, which do not require a physical trespass to be used effectively.[90] He cautioned that such advances in technology invade privacy more than ever.[91]

A significant difference between Justice Alito's approach and the majority's approach has to do with the effect of the *Katz* test.[92] Justice Alito claimed that the *Katz* test replaced the physical trespass approach, whereas the majority claimed it just supplemented the approach.[93] Employing the *Katz* test, Justice Alito explained how the majority opinion ignored the negative implications of long-term tracking without a physical trespass.[94] He claimed that such long-term monitoring infringes upon a person's reasonable expectation of privacy under the *Katz* test.[95] However, Justice Alito did not explain where he would draw the line.[96] How long is long-term?

---

82. *Id.* at 955.
83. *Id.* at 957.
84. *Id.*
85. *Id.*
86. *Id.* (Alito, J., concurring).
87. *Id.* at 953.
88. *Id.* at 958.
89. *Id.*
90. *Id.* at 962.
91. *Id.*at 964.
92. *Id.* at 961.
93. *Id.*
94. *Id.*
95. *Id.* at 964.
96. *Id.*

Although Justice Alito claimed four weeks of surveillance with electronic equipment may cross the line of what constitutes a search and what does not, the facts of the case did not require the court to answer that question.[97] He recognized that the majority's approach essentially permits long-term tracking, so long as the government does not physically trespass on any protected property.[98] Justice Alito expressed his concern regarding the grave danger this posed.[99] The circuit court case law following *Jones* confirmed his fears.[100]

Justice Alito further elaborated on how trivial the court's holding was.[101] Using the majority's rationale, if the government attached a GPS device to the vehicle and tracked the movements for one day, then a search within the meaning of the Fourth Amendment occurred.[102] However, under the majority's approach, if the government did not attach the device, but rather, had the police follow Jones for a long period of time, no search would have occurred.[103] The majority's approach turned on the simple placement of a small device on the vehicle.[104]

To enhance his argument, Justice Alito explained some of the ways the government can track one's location without a physical trespass.[105] For example, he acknowledged that wireless providers can track and record the location of cellular devices.[106] Under the majority's approach, the government is permitted to obtain this information for an extended period without probable cause and a warrant, so long as no physical trespass takes place.[107]

Under the majority's framework, with 322 million wireless phones used in the United States, law enforcement's use of highly advanced surveillance technology to obtain location information gravely diminishes privacy.[108] Due to the nature of modern cell phones and the frequency in which they travel to and from potentially private places with individuals, law enforcements' use of noninvasive, cell site simulators to discover location information triggers the protections of the Fourth Amendment, thereby requiring probable cause and a warrant.

97. *Id.*

98. *Id.* at 961.

99. *Id.* at 955.

100. *See infra* Part III (explaining how circuit courts are employing the *United States v. Jones* holding and reaching contradictory conclusions).

101. *Jones*, 132 S. Ct. at 961 (Alito, J., concurring).

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.* at 962.

106. *Id.* at 963.

107. *Id.*at 962.

108. *Id.*at 963.

III. CIRCUIT COURTS' SPLIT RESPONSE TO *UNITED STATES V. JONES*

In response to *Jones*, circuit courts struggled to apply its holding and dicta.[109] Since *Jones* did not address a pressing question, unsurprisingly, a circuit split arose regarding whether one voluntarily discloses his or her location when utilizing a cell phone.[110]

Section A discusses *United States v. Skinner*, decided shortly after *Jones*, where the Sixth Circuit held that Skinner did not have a reasonable expectation of privacy in location information emanating from his cell phone.[111] Section B discusses *In Re U.S. for Historical Cell Site Data*, where the Fifth Circuit held that the third-party doctrine applies to cell phone users because they knowingly and voluntarily disclose their phone's location information by using their phone.[112] Section C discusses the vacated opinion of *U.S. v. Davis*, where the Eleventh Circuit adopted a contrary approach to the Fifth Circuit and held that a person does not voluntarily disclose his or her location information by using a cell phone. [113] Finally, Section D discusses the holding in *United States v. Graham*, where the Fourth Circuit rejected the notion that cell phone users voluntarily disclose their location when they turn on a cellular device and use it in today's society.[114] The Fourth Circuit held that such information is constitutionally protected under the Fourth Amendment.[115] In effect, this holding supports the notion that law enforcement's use of noninvasive, cell site simulators to discover location information constitutes a search within the meaning of the Fourth Amendment, thereby requiring probable cause and a warrant.

A. United States v. Skinner

Skinner used a "pay-as-you-go phone" that, unbeknownst to him, came with GPS technology to conduct operations pertinent to transporting illegal drugs.[116] Suspecting that Skinner was involved in a large-scale drug trafficking operation, the government "pinged" his cell phone in order to discover Skinner's location

109. *See infra* Part III (explaining the circuit split between the Sixth, Fifth, Eleventh, and Fourth Circuit because of the issue left unanswered in *Jones*).

110. *Id.*

111. *See infra* Part III.A (discussing the Sixth Circuit's approach to the question left unanswered in *Jones*).

112. *See infra* Part III.B (discussing the Fifth Circuit's approach to addressing the question left unanswered in *Jones*).

113. *See infra* Part III.C (discussing the Eleventh Circuit's analysis regarding whether a person voluntarily discloses his or her location information to third parties when using a cell phone).

114. *See infra* Part III.D (discussing the Fourth Circuit's analysis regarding whether a person voluntarily discloses his or her location information to third parties when using a cell phone).

115. United States v. Graham, 796 F.3d 332, 344-45 (4th Cir. 2015).

116. United States v. Skinner 690 F.3d 772, 775 (6th Cir. 2012).

and track his movements over a three-day period.[117] As a result, the police uncovered Skinner's location as he transported drugs across state borders.[118] After the police obtained the cell phone's location, they located Skinner and his son with a motorhome containing over 1,100 pounds of marijuana.[119] Skinner moved to suppress the marijuana on the grounds that the police conduct, leading to its discovery, violated the Fourth Amendment.[120] The district court denied the motion and convicted Skinner of two counts "related to drug trafficking and one count of conspiracy to commit money laundering."[121]

Holding that there was no Fourth Amendment violation, the Sixth Circuit relied on the idea that a cell phone is a modern luxury.[122] It reasoned that if criminals utilize modern technology while engaging in criminal activity, criminals "can hardly complain when police take advantage of the inherent characteristics of those very devices to catch them."[123] The court concluded that Skinner did not have a reasonable expectation of privacy in the "data emanating from his cell phone," which ultimately disclosed his location to the police.[124]

B. In Re Application of the United States for Historical Cell Site Data

In *In Re Application of the United States for Historical Cell Site Data*, the court took a similar approach to that in *Skinner*. In October of 2010, the government filed three applications under the Stored Communications Act[125] to compel cell phone service providers to turn over historical cell-site information for certain cell phones over a 60-day period.[126] Although the government met the specific and articulable facts standard set forth in the Stored Communications Act, the magistrate judge denied the application for historical cell site information.[127] The magistrate judge held that, in light of cell phone technology and based on Supreme Court precedent, "compelled warrantless disclosure of cell site data violates the Fourth Amendment."[128]

---

117. *Id.* at 776.

118. *Id.* at 774.

119. *Id.*

120. *Id.* at 776.

121. *Id.* at 775.

122. *Id.*

123. *Id.* at 774.

124. *Id.*at 775.

125. Stored Communications Act 18 U.S.C.S. § 2703(d) (2016) (permitting the government to gain access to cell site information from cell-phone subscribers if the government has "specific and articulable facts" to support the request rather than probable cause).

126. *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013).

127. *Id.*

128. *Id.*

The government submitted a brief to the district court, and although there was no adverse party to the Government's ex parte application, the American Civil Liberties Union (ACLU) was among the group that participated as *amici curiae*.[129] As a result, the ACLU raised a constitutional challenge to the Stored Communications Act.[130] The district court concluded that the government could only request location information from cell phone providers if it obtained a warrant based on probable cause.[131] The district judge based this holding on the rationale that when someone places a call, his or her location information and other data is constitutionally protected. Deeming the statute unconstitutional, the district court's holding supports the notion that one does not voluntarily disclose his or her location to the service provider when using a cell phone.[132]

The ACLU argued that the government's action of gaining access to cell site records, reflecting activity over a 60-day period, undoubtedly violates an individual's reasonable expectation of privacy under *Katz*.[133] Using the notion from Justice Alito's concurring opinion in *Jones* to support this argument, the ACLU reasoned that obtaining the cell site records for over a 60-day period crossed the line.[134] Enhancing this argument, the ACLU analogized the car in *Jones* to the cell phone.[135] Since most people carry their cell phones on their person everywhere they go, tracking the movements of the device is much more invasive and reveals much more sensitive information than tracking the movements of a vehicle, which people only use for the purpose of getting to and from a certain destination.[136]

The court disagreed with the ACLU, and held that the third-party doctrine applied in this situation by drawing the distinction between business records and the communications' content, such as tracking information.[137] Since the court classified the cell site information as a business record maintained and stored by the service providers, the government argued, and the court agreed, that cell phone users knowingly disclose their location information to their service providers when they voluntarily make phone calls.[138] This argument relies on the notion that all cell phone users understand the way in which their phones operate.[139]

---

129. *Id.*
130. *Id.* at 603.
131. *Id.*
132. *Id.*
133. *Id.* at 608.
134. *Id.*
135. *Id.*at 609.
136. *Id.*
137. *Id.* at 611.
138. *Id.* at 612.
139. *Id.* at 613.

The dissent in *In re Application of the United States for Historical Cell Site Data* embraces the notion that the Supreme Court's decision in *Jones* forces lower courts to "venture onto uncertain terrain" in applying the *Katz* analysis to these law enforcement practices.[140] Elaborating on the three separate opinions in *Jones*, Judge Dennis disagreed with the majority's rationale because he deemed historical cell site location information as potentially protected information under the Fourth Amendment.[141] He argued that since the information is constitutionally protected, the statute requires the government to obtain a warrant before compelling such information from service providers.[142] The dissent based its conclusion on the nature of the cell site location information.[143]

C. United States v. Davis

United States v. Davis presented the Eleventh Circuit with the same issue that the Fifth Circuit decided one year earlier.[144] In *Davis*, the defendant, Davis, was charged with "conspiracy to engage in Hobbs Act Robbery" and with "knowingly using, carrying, and possessing a firearm in furtherance of a crime of violence."[145] Witnesses testified that Davis was involved in various robberies where the participants all wore masks and carried weapons in an attempt to steal miscellaneous items and cash.[146] Along with testimony explaining Davis' role in each robbery, the prosecution also offered evidence that Davis and his co-defendants made and received phone calls near the location of each robbery around the approximate time of the robberies.[147]

Davis moved to suppress the cell site location information that the government obtained without a warrant on the grounds that it violated his Fourth Amendment rights when the prosecution attempted to introduce it at trial.[148] The district court denied Davis' motion and the jury convicted Davis on all counts.[149] On appeal, Davis argued the district court erred in denying his motion to suppress the cell site location information.[150] Davis argued that the Fourth amendment protects cell site location information.[151] As a result, he argued that obtaining

140. *Id.* at 624 (Dennis, J., dissenting).

141. *Id.*

142. *Id.* at 629.

143. *Id.* at 632.

144. *See* United States v. Davis, 754 F.3d. 1205 (11th Cir. 2014) (addressing whether the government needs probable cause and a warrant in order to obtain cell site location information), *vacated*, No. 12–12928, 573 Fed.App'x. 925 (Fla. L. Weekly Supp. 2014).

145. *Id.* at 1209.

146. *Id.*

147. *Id.* at 1209–10.

148. *Id.* at 1210.

149. *Id.*

150. *Id.*

151. *Id.* at 1211.

such information requires probable cause and a warrant.[152] However, the government argued that such information is not protected by the Fourth Amendment and can be obtained under a court order pursuant to the Stored Communications Act.[153]

Recognizing the Supreme Court has yet to decide the issue, the Eleventh Circuit still used the holding in *Jones* to formulate its opinion.[154] The court began by analyzing the police conduct. In *Davis*, the government obtained the location information pursuant to the Stored Communications Act.[155] Cell site location information makes it possible to discover the location of the user at a particular time because it contains his or her direction from cellular towers.[156]

In *Davis*, the government obtained location information using technology without committing a physical trespass. The *Jones* court explained situations absent a physical trespass "remain subject" to the *Katz* test. Operating under the *Katz* framework, the Eleventh Circuit explained that the Fourth Amendment protects people from "warrantless interception of electronic data or sound waves carrying communication."[157] However, it remains unanswered whether the projection extends to the transmission alone, not revealing content of communications but revealing location information of the source of the transmission.[158]

The court explained that although *Jones* used the trespass theory to find a constitutional violation, it recognized the notion that electronically transmitted location information can be protected by the Fourth Amendment.[159] Analyzing the separate opinions in *Jones*, the court in *Davis* concluded that this was an instance where the Fourth Amendment protects electronically transmitted location information.[160] Therefore, *Davis* held that the government violated Davis' reasonable expectation of privacy when it gathered his cell site location information without probable cause and a warrant.[161]

The court used the premise adopted by the Third Circuit to explain its reasoning.[162] In *In re Electronic Communications Service to Disclose*, the Third Circuit explained that a cell phone customer does not voluntarily disclose location information to his or her cell phone provider "in any meaningful way" as to relinquish his or her reasonable expectation of privacy.[163] The court based its

152. *Id.*
153. *Id.*at 1214.
154. *Id.*
155. *Id.* at 1210.
156. *Id.* at 1211.
157. *Id.* at 1213.
158. *Id.* at 1215.
159. *Id.*
160. *Id.* at 1215.
161. *Id.*
162. *Id.* at 1216–17.
163. *Id.* at 1217.

holding on the disbelief that cell phone users are even aware that their providers store such information.[164]

Adopting the Third Circuit's premise, that one does not voluntarily disclose location information by making a phone call, the court made the even more persuasive argument that one does not voluntarily convey anything whatsoever when they receive a call.[165] The court did not find any support for the idea that by simply placing or receiving a call, the caller is subsequently conveying his or her location to anyone. The Third Circuit found the third-party doctrine inapplicable on these facts and concluded that the government must seek a warrant before obtaining cell site location information.[166]

D. United States v. Graham

Finally, in 2015, the Fourth Circuit decided *United States v. Graham*.[167] In *Graham*, Graham was convicted of "being a felon in possession of a firearm, Hobbs Act Robbery, conspiracy to commit Hobbs Act robbery, and brandishing a firearm in connection with all six robberies."[168] The government obtained cell site location information from Sprint for a 221 day period as part of its investigation of the robberies.[169] The cell site location information revealed that the defendants were in close proximity to most of the robberies before and after each robbery took place.[170]

The government obtained a court order for this information under the Stored Communications Act.[171] As a result, the defendants filed a motion to suppress the use of this information at trial because the government obtained this information without probable cause and a warrant.[172] However, the district court denied the motion because the government did not conduct an unreasonable search prohibited by the Fourth Amendment.[173] The defendants appealed to the Fourth Circuit.

The Fourth Circuit found the third-party doctrine inapplicable.[174] The court compared the police conduct in this case to long-term GPS monitoring, which reveals intimate details of a person's life based on his or her location.[175] It reasoned that a cell phone user does not voluntarily convey his or her location

164. *Id.*
165. *Id.*
166. *Id.*
167. United States v. Graham, 796 F.3d 332, 332 (4th Cir. 2015).
168. *Id.* at 339.
169. *Id.*
170. *Id.* at 342–43.
171. *Id.* at 344.
172. *Id.* at 342.
173. *Id.*
174. *Id.* at 345.
175. *Id.* at 348.

information because a cell phone is constantly conveying this data even when it is not in use. The nature of a cell phone played a large role in the court's holding.[176]

Analogizing the searches in *Kyllo* and *Karo* to the cell site location information, the court explained that the government can locate an individual at his or her home along with other private places and not just on public roads.[177] Here, since one usually carries the cell phone on one's person, the location information discloses the whereabouts of a particular individual rather than the location of an object, such as a container of Chloroform.[178] Further, over 221 days, the appellant was without a doubt home on many occasions, which is the most sacred protected place under the Fourth Amendment since the adoption of the amendment itself. Simply because technology has made it possible for a citizen to carry this device that is capable of revealing location information on his or her person does not make it any less unworthy of protection under the Fourth Amendment.[179] As a result, the court held that the police action amounts to a search under the Fourth Amendment, requiring probable cause and a warrant.[180]

Judge Thacker concurred;[181] she reasoned that the third-party doctrine did not apply because as advances in technology emerge, privacy rights diminish at the same pace.[182] As a result, "each step forward should be met with considered judgment that errs on the side of protecting privacy and accounting for the practical realities of modern life."[183] She also stated that a different outcome permits the government to force service providers to turn over location information without probable cause.[184] Such a notion is preposterous if there is anything left to the protection of the Fourth Amendment. Her argument is centered on the way in which modern cell phones work. She believes it is "disturbing" that American citizens can be "tracked from afar regardless of whether or not [they] are actively using [their] phones."[185]

Judge Motz dissented in the judgment on the basis that *stare decisis* permitted the police conduct in this particular case without the need of probable cause and a warrant.[186] The dissent believed the third-party doctrine was controlling on these facts, which meant the protections of the Fourth Amendment were not triggered.[187] Judge Motz analogized the collecting of the location

176. *Id.* at 378.
177. *Id.* at 346.
178. *Id.* at 348.
179. *Id.* at 378.
180. *Id.* at 360–61.
181. *Id.* at 377 (Thacker, J., concurring).
182. *Id.*
183. *Id.* at 378.
184. *Id.*
185. *Id.*
186. *Id.* (Motz, J., dissenting).
187. *Id.* at 380.

information in *Graham* to the dialed numbers recorded by the pen register in *Smith*, and found that the government's action did not constitute a search within the meaning of the Fourth Amendment.[188]

IV. TACKLING THE SPLIT: WHY THE FOURTH CIRCUIT GOT IT RIGHT

Without adopting the Fourth Circuit's holding in *Graham*, the Supreme Court enables law enforcement to use advances in technology to erode the protections of the Fourth Amendment. To ensure advances in technology do not deplete privacy protections guaranteed by the Fourth Amendment, law enforcement use of noninvasive, cell site simulators to discover location information must constitute a search within the meaning of the Fourth Amendment, thereby requiring probable cause and a warrant.

Section A illustrates the types of devices law enforcement officers currently use in criminal investigations to discover an individual's location information.[189] Section B discusses the flaws in the Fifth and Sixth Circuit's contrary approach as compared to the Fourth Circuit's holding, and the dangers posed by unregulated use of cell site simulators.[190] Section C discusses a pending lawsuit against the Sacramento, California, Police Department for its warrantless use of these problematic devices.[191]

A. Cell Site Simulators: Stingray, Triggerfish, Amberjack, Kingfish, and Loggerhead Devices

Devices used by the government during the course of its criminal investigation designed to gain access to location information are plentiful and consequently many of them fall outside the scope of existing statutory regulations.[192] Although Congress has not expressly permitted the use of these technologically-advanced devices, the government utilizes holes in current legislation and the Fourth Amendment framework to use them anyway.[193] Amongst the most common of these devices are cell-site simulators. These

188. *Id.*

189. *See infra* Part IV.A (illustrating the types of devices law enforcement officers currently use in criminal investigations to discover individual's location information such as cell site simulators).

190. *See infra* Part IV.B (discussing the flaws in the Fifth and Sixth Circuits' holding that one voluntarily conveys his or her location information to his or her service provider when using a cell phone).

191. *See infra* Part IV.C (explaining the current lawsuit pending against the Sacramento Police Department for its use of Stingray devices).

192. Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 143 n.2 (2014).

193. *Id.*

simulators are called many different names including "stingray," "triggerfish," and "kingfish."[194]

Many people may have heard of these devices but have no idea how they actually work. The reason for that is because many law enforcement officers and even the manufacturer of these devices, the Harris Corporation, want to keep the use of these devices concealed from the public.[195] The Harris Corporation even goes so far as to require law enforcement officials to sign non-disclosure agreements before using the devices.[196] What are they so desperate to hide? The answer lies within the extremely intrusive way these devices operate and the devices' ability to reveal sensitive location information at the push of a button.[197] These devices essentially transform "a piece of technology so ubiquitous as to be on the person of practically every citizen" into a real-time tracking device.[198]

When the government activates the devices, all of the cell phones in the same geographical area send information directly to those devices. Because cell-phones use cell towers to "transmit data,"[199] these devices can "trick" the cell phones into thinking the device is a cell tower, which allows the device to trap the cell phone's metadata.[200] This metadata includes, amongst a plethora of information, the location of the cell phone, which as a result, reveals the real time location of the cell phone user. By acting as a cell phone tower, these devices force the cell phone to send a responding signal to the device.[201] If the device is within the cell phone's signal range, it can measure signals from the phone, and in light of the signal strength, the device reveals the location of the phone.[202] By repeating this and by "collecting the cell phone's signals from several locations," the device can "develop the location of the phone quite precisely."[203]

194. *In re* United States, No. 15M0021, 2015 U.S. Dist. LEXIS 151811, at *7 (Ill. Cir. Ct. Nov. 9, 2015).

195. *Id.* at *2.

196. *Id.*

197. *Id.* at *7.

198. State of Maryland v. Andrews, No. 1496, 2016 WL 1254567, at *1 (Md. Ct. Spec. App. March 30, 2016)

199. Marissa Lang, *The Sacramento County Sheriff's Department sued over 'Stingray' Surveillance Technology*, THE SACRAMENTO BEE, Mar. 10, 2015.

200. *Id.*

201. State of Maryland v. Andrews, No. 1496, 2016 WL 1254567, at *14.

202. *Id.*

203. *Id.* at *14.

The following chilling conversation highlighted in *Andrews* brings the highly invasive nature of these devices to life:

> [DEFENSE COUNSEL]: Okay. And so, if a person is inside of a home, that equipment peers over the wall of the home, to see if that cell phone is behind the wall of that house, right?
>
> [DETECTIVE HALEY]: Yes.
>
> [DEFENSE COUNSEL]: And it sends an electronic transmission through the wall of that house, correct?
>
> [DETECTIVE HALEY]: Yes.[204]

B. Failing to Recognize the Nature of Modern Cell Phones is Eroding Privacy Rights

The argument in *Skinner*, that criminals should not complain when police take advantage of the "inherent characteristics" of modern technology to "catch them," may at first glance seem persuasive.[205] However, the reality that the guilty might benefit from constitutional protections and sometimes "go free" because the Fourth Amendment conceals incriminating evidence is not a new phenomenon.[206] Although some believe the guilty do not deserve the constitutional rights, and criminals should not benefit from Fourth Amendment protections, many constitutional rights are in place to protect the accused.[207] Those fearful that criminals using modern technology to partake in criminal activity will benefit from requiring law enforcement to obtain a warrant before using cell site simulators to access location information, "are not to be aided by the sacrifice of those great principles established by years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land."[208] In other words, suppressing evidence that is needed to convict the guilty is the price the legal system pays to protect the rights of the innocent from arbitrary police conduct while preserving the principles underlying the Fourth Amendment.

---

204. *Id.* at 5.

205. United States v. Skinner, 690 F.3d, 772, 772 (6th Cir. 2012).

206. *See* Mapp v. Ohio, 367 U.S. 643, 648 (1961) (introducing the exclusionary rule).

207. *See* U.S. CONST. amend. V (providing no person shall "be deprived of life, liberty, or property, without due process of law"); *id.* amend. VI (explaining "the accused shall enjoy the right to a speedy and public trial, by an impartial jury"); *id.* amend. VIII (prohibiting cruel and unusual punishment and excessive bail).

208. *Mapp*, 367 U.S. at 648.

Further, by classifying cell phones as "modern luxuries," the court in *Skinner* failed to recognize the nature of cell phones in today's society.[209] Modern cell phones are hardly "another technological convenience" as *Skinner* stated.[210] Rather, they contain "the privacies of life" for many similar to those contained in one's home or office.[211]

Like *Skinner*, the Fifth Circuit in *In re Application of the United States for Historical Cell Site Data* ignored the modern realities surrounding the cell phone.[212] While all users may understand that their phone must send signals to cell towers in order to make phone calls, which is then received by the service provider, it would be ridiculous in today's society to argue that by doing so and by simply understanding the mechanics of a cell phone's ability to place calls, a person is subsequently relinquishing all privacy rights as to his or her location when they place a call. This is so because a modern cell phone is much more than just a telephone.

As Chief Justice Roberts explained, "the term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[213] This is true because the nature of cell phones has evolved dramatically over time. Modern cell phones can store an immense amount of data including, but definitely not limited to, photographs, emails, notes, and financial information.[214] This large storage capacity allows a person to carry around the most telling and intimate information about them that was once physically impossible.[215]

Another problematic argument is one the Fifth Circuit employed. The Fifth Circuit elaborated on the notion that using a cell phone is entirely voluntary.[216] However, in a world dominated by technology, this is no longer the case. In a world where 90 percent of American adults own cell phones, an active member of society must own one as well.[217] This is hardly a choice. On this note, the court makes the additional argument that the government does not require a person to own a cell phone.[218] This argument is naïve and ignores blatant flaws in such an assertion.[219]

---

209. *Skinner*, 690 F.3d at 772.

210. Riley v. California, 134 S.Ct. 2473, 2494 (2014).

211. *Id.*at 2495.

212. *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 609 (5th Cir. 2013) (holding one does not have a reasonable expectation of privacy in his or her location information disclosed through the use of his or her cell phone).

213. *Riley*, 134 S.Ct. at 2489.

214. *Id.*

215. *Id.* at 2490.

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

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

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

219. *Id.*

The court also argues that the government does not require a person to make a phone call at a specific location if he or she does not want his or her location information to be revealed.[220] But in the case of the emergency phone call, does a person really have a choice? If an individual is receiving an emergency phone call while visiting a location he or she perceives as private, the Fifth Circuit provides two options. The person can either ignore the call or relinquish any privacy rights he or she may have over his or her location when answering the call.[221] In today's world, this should not be a choice one has to make.

The ACLU persuasively argued that advances in technology change society's reasonable expectation of privacy.[222] The Fifth Circuit agreed with the ACLU, but explained that a diminution in privacy is an inevitable tradeoff to technological advances.[223] It is frightening to conceive of the fact that the Fifth Circuit is openly accepting the notion that its holding erodes privacy rights that are deeply embedded in Fourth Amendment jurisprudence. If this type of government surveillance escapes the bounds of the Fourth Amendment, as the Fifth Circuit enables it to, society will experience similar diminished privacy rights to those the citizens in the 1580s faced when courts issued general warrants.[224]

General warrants were "indefinite" and provided those executing them with "limitless" authority to search and seize whatever they please.[225] The warrant executors ransacked homes to obtain incriminating evidence.[226] Because the vast majority of Americans own cell phones, allowing the government to exploit the nature of these devices essentially permits it to obtain a general warrant to access each and every American's location at any given time.[227] Since modern cell phones have such a large storage capacity, they can contain important, private information that was once only held within the confines of one's home.[228] To avoid the unwanted general warrant effects, the Supreme Court must recognize that the use of cell site simulators implicate Fourth Amendment protections.[229]

When the Eleventh Circuit faced the same issue, it disagreed with the conclusions the Fifth and Sixth Circuit came to and based its holding on the fact that one does not voluntarily disclose location information to a third-party provider by owning a cell phone.[230] However, the court vacated its holding soon

220. *Id.*

221. *Id.*

222. In re *Application of the United States for Historical Cell Site Data*, 724 F.3d at 614.

223. *Id.*

224. Cuddihy, *supra* note 26 at 998.

225. *Id.*

226. *Id.*

227. *See id.*(discussing the adverse effects of general warrants).

228. *Riley*, 134 S.Ct. at 2491.

229. In re *Application of the United States for Historical Cell Site Data*, 724 F.3d at 630- 31.

230. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014).

after.[231] Although the Eleventh Circuit is rehearing the case, the analysis conducted in the opinion is worth noting. It is in tune with modern realities and Supreme Court precedent. The Eleventh Circuit recognizes that the only information voluntarily conveyed to the phone company when a person places a call is the numbers dialed.[232] Adopting this approach will help curb arbitrary police activity.

The Fourth Circuit's approach is most reflective of modern realities, and preserves the sanctity of the Fourth Amendment.[233] In *Graham,* the court correctly highlighted the notion that obtaining cell site location information is much more than simply using a pen register to obtain numbers dialed.[234] Collecting and storing location information is a feature embedded in many smart phones and is enabled automatically when a phone activates.[235] Contrary to physically pressing the buttons on a phone to make a phone call, where one is conveying numbers dialed to his or her provider, by simply possessing a phone and standing idly by it, one is not voluntarily conveying anything to anyone. Obtaining this information reveals a person's specific movements "down to the minute."[236]

Although the dissent believes the majority in *Graham* is attempting to "beat the Supreme Court to the punch," the Supreme Court left lower courts with little guidance on how to decide the issue and instead of ignoring the issue, they used the dicta throughout *Jones* in an attempt to decide the case.[237] Without direct precedent on point and in light of modern realities, the court used common sense and focused on the nature of smart phones in 2016. However, the dissent compellingly pointed out that the Supreme Court needs to revisit the third-party doctrine and address the long-term cell site location information issues to eliminate the blatant inconsistencies among the circuit courts' rulings.[238]

C. The Stingray's Harsh Sting

Because these modes of surveillance are much more invasive than those used in *Knotts*, *Karo*, *Kyllo*, and *Smith*, the nature of the information they can potentially reveal is much more private.[239] In *Kyllo*, Justice Scalia acknowledged the fact that, "it would be foolish to contend that the degree of privacy . . . has

231. *Id.*; *See* U.S. v. Davis, 573 Fed.Appx. 925, 925 (11th Cir. 2014) (granting rehearing en banc and vacating U.S. v. Davis).

232. *Id.* at 1217.

233. *See* United States v. Graham, 796 F.3d 332, 378 (4th Cir. 2015) (discussing the amount of information available in cell phones).

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.* at 390.

238. *Id.* at 389–90.

239. *See id.* at 378 (describing the amount of information accessible).

been entirely unaffected by the advance of technology."[240] Justice Scalia phrased the issue broadly and explained that the Court in *Kyllo* had to decide "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[241] Cell site simulators reveal, among other information, location data.[242] On the other hand, the use of a beeper in *Knotts* only revealed Knotts' movements on public roadways.[243] While a person driving a car on public roadways anticipates the public seeing his movements, a person does not anticipate the public seeing his movements when carrying a cell phone or that the cell phone is being used as a tracking device.[244]

In *Jones*, Justice Alito argued that long-term monitoring of a vehicle's movements can violate a person's reasonable expectation of privacy.[245] The Eleventh Circuit accurately explained that when dealing with cell site location information, an aggregation of movements over a lengthy period of time is not necessary to establish the invasion of privacy.[246] Because "one's cell phone, unlike an automobile, can accompany its owner anywhere, the exposure of the cell site location information can turn a 'private event into a public one.'"[247] Recognizing that Justice Alito's concurring opinion in *Jones* stood for the proposition that GPS location information on an automobile is protected only in the case of "aggregated data," one may have a reasonable expectation of privacy over one point of cell site location information.[248]

Comparing cell site data to communications, which are protected by the Fourth Amendment, the Court explained that the information is inherently private.[249] In *Davis*, the court explained the cell site information used by the government placed Davis near all of the robberies.[250] The private nature of the information is illustrated by the reality that the government's action could have placed him "near the home of a lover, or a dispensary of medicine, or a place of worship, or a house of ill repute."[251]

Like *Karo*, obtaining location information can place someone inside his or her home, the most sacred, protected place under the Fourth Amendment. In *Andrews*, the government, using a cell site simulator, obtained Andrews' location and found Andrews seated on the couch in his living room with his cell phone in

240. Kyllo v. United States, 533 U.S. 27, 34–35 (2001).
241. *Id.*
242. *Graham*, 796 F.3d at 378.
243. United States v. Davis, 785 F.3d 498, 521, n.1 (11th Cir. 2015).
244. United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014).
245. United States v. Jones, 132 S. Ct. 945, 958 (2012).
246. *Id.*
247. *Id.*
248. *Id.*
249. *Id.*
250. *Davis*, 754 F.3d at 1217.
251. *Id.*at 1216.

his pants pocket.[252] Although using these devices to track a phone will not always result in locating the phone in a home, "the government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces."[253]

Since it is impossible for law enforcement to determine before using the various devices to obtain the cell phone user's location information whether the user will be in a constitutionally protected area, it is crucial to focus on the nature of information that can potentially be disclosed.[254] Requiring probable cause and a warrant before employing these devices will protect the private, sensitive information that could be revealed.[255]

In *Smith*, the government used a pen register to discover the numbers Smith dialed.[256] A pen register does not reveal contents of communications.[257] Although cell site simulators technically do not reveal contents of communications either, the devices can reveal a cell phones' location and subsequently, a person's exact whereabouts.[258] The ability to obtain location information is more analogous to obtaining content of communications rather than simply numbers dialed. Through the use of these devices, the government is able to determine the cell phone user's location, wherever that may be.[259]

Because of the unregulated use of these devices, anywhere people travel with their cell phone cannot be kept private. These devices accumulate intimate information about any person the government chooses to track, which has the potential to "alter the relationship between citizen and government in a way that is inimical to democratic society."[260] The use of such technology has led to lawsuits and unease among citizens.

252. Andrews, No. 1496, 2016 WL 1254567, at *1 (Md. Ct. Spec. App. 2016) (holding the government's use of a cell site simulator was a search within the meaning of the Fourth Amendment because Andrews did not voluntarily disclose his cell site location information with his cell phone provider so he had a reasonable expectation of privacy in his cell phone location information).

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

254. *In re* Application of United *States* for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F.Supp.2d 526, 540 (D. Md. 2011).

255. *See* Andrews, No. 1496, 2016 WL 1254567 at *16 (Md. Ct. Spec. App. 2016) (illustrating how use of a cell site simulator allowed police to locate Andrews within his home).

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

257. *Id.*

258. United States v. Graham, 796 F.3d 332, 378 (4th Cir. 2015).

259. *Id.*

260. United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S.Ct. 1534 (2012).

D. Taking a Stand Against the Use of These Devices: Refusing to Get Stung by the Stingray

Efforts to hide the use of these devices are slowly unraveling and citizens are no longer standing idly by now that they are finally aware of these law enforcement surveillance techniques. For example, in March 2015, the ACLU sued the Sacramento County Sheriff's Department for the department's use of the Stingray device.[261] The department assures the Sacramento community that it uses such devices infrequently in "special" circumstances.[262] How does the public know where the department draws the line? Using these devices in "special" circumstances without probable cause and a warrant creates a slippery slope and no guidance for lower courts when deciding what police activity to condemn and condone.[263] It also provides no guidance to police departments when deciding in which circumstances to use these devices.

Courts are best equipped to determine where the line should be drawn rather than the police, who have little incentive to draw lines, limiting its ability to employ these devices. If the Supreme Court requires probable cause and a warrant to use cell site simulators to obtain cell site location information, there will be no ambiguity as to when these devices can be employed. Law enforcement will not be forced to make a judgment call and citizens will be at ease knowing these devices are employed only after police follow proper procedures to obtain a warrant.

Further, in Sacramento, the local authorities refused to disclose information about the use of these devices, which would better the community's understanding of them.[264] The public has the right to know the extent to which these highly invasive devices are infringing upon their privacy and constitutional rights guaranteed by the Fourth Amendment, and the consequences that using cell phones may have on their expectation of privacy in their location.[265]

Following the Fourth Circuit's stance, and adopting the premise that a person does not voluntarily disclose his or her location information when owning and operating a cell phone, would require the police to obtain a warrant based on probable cause before employing these techniques.[266] This is not to say police can no longer utilize these highly effective devices, it is simply ensuring that the Framer's intention when creating the Fourth Amendment is not completely obliterated through the use of such devices. It will ensure Fourth Amendment protections do not stand still as technology continues to advance.

---

261. Lang, *supra* note 199 (elaborating on the allegations the Sacramento County Police Department faces surrounding its use of the Stingray).

262. *Id.*

263. *Id.*

264. *Id.*

265. *Id.*

266. *Graham*, 796 F.3d at 344.

V. CONCLUSION

In the past, the protections of the Fourth Amendment were centered on preserving the sanctity of the home. However, today "a cell phone search would typically expose to the government far more than the most exhaustive search of a house."[267] At a minimum, the Fourth Amendment should protect the same sacred information it sought to protect when it was adopted, regardless of whether the information is in a home or contained in a cell phone. In a society where 90% of American adults own and use cell phones, adopting the Fifth Circuit's approach that one voluntarily discloses his or her location information to his or her third-party provider, means 90% of American adults relinquish any reasonable expectation of privacy over their whereabouts essentially at any given time.

Until the Supreme Court addresses this issue, the government is free to continue employing these devices without probable cause and a warrant.[268] Requiring the government to obtain a warrant before using these devices will preserve the protections guaranteed by the Fourth Amendment without overburdening law enforcement, since exceptions to the warrant requirement are few and far between.

Advances in technology continue to flourish. The negative implications of not addressing this issue are enormous.[269] Among those negative implications includes the feeling of being constantly watched or under 24-hour surveillance. As Justice Douglas bluntly put it, "We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government."[270] Without revisiting the question left unanswered in *Jones*, the Supreme Court allows law enforcement to expose the gap in Fourth Amendment case law through advanced surveillance techniques.[271] Until this question is answered—Big Brother is watching!

267. Riley v. California, 134 S.Ct. 2473, 2497 (2014).

268. *Supra* Part IV (arguing why the Fourth Circuit's approach was correct).

269. *Supra* Part IV (illustrating the issues surrounding advanced technology and the negative implications of not addressing them).

270. Andrews, No. 1496, 2016 WL 1254567 at *16 (Md. Ct. Spec. App. 2016).

271. *Supra* Part IV (arguing the harm resulting from the Supreme Court's failure to revisit the question left unanswered in *Jones*).