CELL PHONE TRACKING IN THE ERA OF *UNITED STATES V. JONES* AND *RILEY V. CALIFORNIA*

Brian L. Owsley[*]

Cell phones have become ubiquitous in American society. Some estimates are that, as of 2013, about 91% of adults in the United States had a cell phone.[1] Indeed, almost two-thirds of cell phone users sleep with a cell phone on their bed or right next to it.[2] The Supreme Court has commented on the ubiquitous nature of cell phones and other electronic devices.[3] In other

---

* Assistant Professor of Law, University of North Texas–Dallas College of Law; B.A., University of Notre Dame; J.D., Columbia University School of Law; M.I.A., Columbia University School of International and Public Affairs. From 2005 to 2013, the Author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The Author expresses his thanks and gratitude to Professor Arnold Loewy and Texas Tech University School of Law for their invitation to participate and present ideas at the 2015 Criminal Law Symposium. The Author also expresses his appreciation for thoughtful editorial suggestions by Melanie Reid.

1. Alexis C. Madrigal, *More Than 90% of Adult Americans Have Cell Phones*, ATLANTIC (June 6, 2013), http://www.theatlantic.com/technology/archive/2013/06/more-than-90-of-adult-americans-have-cell-phones/276615/; Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RES. CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

2. Amanda Lenhart, *Cell Phones and American Adults*, PEW RES. CTR. (Sept. 2, 2010), http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/.

3. Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[C]ell 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."); United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.").

words, for most of us, our cell phones are within reach around the clock.[4] The downside to this extreme intimacy with our phones means that our locations can be tracked based on data emanated from the phones.[5]

A cell phone can be used to track the location of whoever has possession of a cell phone by two distinct means: Global Positioning System (GPS) or cell tower location.[6] Regarding the latter, each cell phone, in order to function, must register frequently with the nearest cell phone towers.[7] While engaging in this registration, the cell phone creates cell site data of two types: historical or real time.[8] Historical cell site data can be used to track the cell phone (and presumably the user) as far back as reliable data exists.[9] In other words, this information can create a line approximating everywhere the user has been in the past, provided that the phone was on the user's person or within their proximity.[10] One court has explained that "[b]y correlating the precise time and angle at which a phone's signal arrives at multiple sector base stations, a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less. Emerging versions of the technology are even more precise."[11] Even though cell site location information (CSLI) does not pinpoint the location of the cell phone (and its user), it is sufficiently accurate that prosecutors rely on it at trial.[12]

Additionally, many cell phones today have GPS capability.[13] This technology utilizes a series of satellites orbiting the Earth in conjunction with hardware in the cell phone that receives data from a number of these satellites, enabling a calculation of the cell phone's longitude and latitude.[14] When that feature is operational, a cell phone can be tracked to its location with a high degree of accuracy.[15] Indeed, a cell phone that does not have its

---

4. *See Riley*, 134 S. Ct. at 2490 (citing a study that found nearly 75% of smart phone users are within five feet of their cell phone at all times).

5. Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH., no. 1, 2011, at 7–8.

6. *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 831–32 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013); *see* Blank, *supra* note 5, at 7.

7. Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 188–89 (2014) [hereinafter Owsley, *TriggerFish*] (stating that registration occurs as frequently as every seven seconds); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 5 (2013) [hereinafter Owsley, *Cell Tower Dumps*] (same).

8. *See* Blank, *supra* note 5.

9. *Id.*

10. *See id.* at 4–6.

11. *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 833; *see also* Blank, *supra* note 5, at 7–10 (describing the methods law enforcement can use to track cell phones).

12. United States v. Davis, 754 F.3d 1205, 1211 (11th Cir. 2014), *reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014) (mem.).

13. *See In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 833.

14. *See id.* at 831; *see also* Blank, *supra* note 5 ("A GPS receiver can track in real-time or make a record of its location with accuracy up to a few meters.").

15. *See* Blank, *supra* note 5.

GPS feature disabled and is not unobstructed from satellites can provide a location within ten meters.[16]

This Article addresses the Supreme Court's recent decisions in *United States v. Jones* and *Riley v. California*, which impact how law enforcement officials may use cell phones as tracking devices. Part I discusses *Jones*, followed by Part II, which addresses *Riley*. Next, Part III outlines the development of the third-party doctrine. Finally, Part IV addresses federal statutes concerning how cell phones are viewed in regards to their tracking capabilities notwithstanding the third-party doctrine.

I. *UNITED STATES V. JONES*

In 2004, the FBI, in conjunction with the District of Columbia police department, began investigating Antoine Jones for drug trafficking, during which time they performed visual surveillance of his nightclub and obtained a wiretap on his cell phone and a pen register.[17] In 2005, federal agents applied for a warrant from the United States District Court for the District of Columbia to place an electronic surveillance device that utilized GPS on a vehicle used by Jones.[18] The warrant was granted, requiring that the police install the device within ten days and in the District of Columbia.[19] The agents waited until the eleventh day, however, and then installed the device on his vehicle in a Maryland public parking lot.[20]

Based on this GPS tracking device, agents monitored the vehicle's whereabouts for twenty-eight days.[21] Using information obtained from the device, they were able to track the vehicle within 50 to 100 feet of its location and relay that information to a computer, resulting in over 2,000 pages of data during the twenty-eight days.[22]

Based in part on this information, Jones and some coconspirators were charged in the United States District Court for the District of Columbia with conspiracy to distribute and possession with intent to distribute more than five kilograms of cocaine and in excess of fifty grams of cocaine base (also known as crack cocaine).[23] Jones filed a motion to suppress evidence obtained from the GPS tracking device.[24] The trial court suppressed evidence obtained while the vehicle was in Jones's garage, but denied the motion as it

16. *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 832; *see also* Blank, *supra* note 5 (describing the proximity from which cell phone location data can be obtained).
17. United States v. Jones, 132 S. Ct. 945, 948 (2012) (majority opinion).
18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*; *see* 21 U.S.C. §§ 841, 846 (2012).
24. *Jones*, 132 S. Ct. at 948.

related to evidence obtained while the vehicle was on public streets because there was no reasonable expectation of privacy in those places.[25]

After Jones's first trial ended without a verdict in October 2006, another grand jury reindicted him and his coconspirators on the same charges in March 2007.[26] The prosecution introduced the same evidence obtained from the GPS tracking device at the second trial, but this time the jury found Jones guilty.[27] The trial judge sentenced him to life in prison.[28]

The United States Court of Appeals for the District of Columbia reversed the conviction, holding that the admitted evidence from the GPS device violated Jones's Fourth Amendment rights.[29] That court then denied the Government's petition for review en banc.[30] The Supreme Court granted the Government's petition for a writ of certiorari.[31] Specifically, the Court addressed whether the use of a GPS tracking device on Jones's vehicle to monitor his movements on public streets violated the Fourth Amendment.[32]

Justice Scalia, writing for the Court in an opinion joined by Chief Justice Roberts as well as Justices Kennedy, Thomas, and Sotomayor, began his analysis by discussing the historical development of the Fourth Amendment.[33] He characterized this case as one in which the Government physically occupied Jones's property to gather information about him in such a physically intrusive manner that the Government's actions constituted a Fourth Amendment search.[34] Justice Scalia stressed that property and individual property rights are central to Fourth Amendment jurisprudence.[35] Next, he discussed how the courts historically tied the Fourth Amendment to principles of common law trespass when there was no search because officers did not enter the defendants' homes or offices.[36] Since 1967, in *Katz v. United States*,[37] the Court has focused on a second test based on an individual's reasonable expectation of privacy instead of the traditional, property-centric test.[38]

---

25. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (relying on United States v. Knotts, 460 U.S. 276, 281 (1983)), *aff'd in part*, *rev'd in part sub nom. Maynard*, 615 F.3d 544; *accord Jones*, 132 S. Ct. at 948.

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

27. *Id.* at 948–49.

28. *Id.* at 949.

29. United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010).

30. United States v. Jones, 625 F.3d 766, 767 (D.C. Cir. 2010) (en banc).

31. United States v. Jones, 131 S. Ct. 3064, 3064 (2011).

32. *Jones*, 132 S. Ct. at 948; *see also* Owsley, *Cell Tower Dumps*, *supra* note 7, at 34–36 (discussing *Jones*).

33. *Jones*, 132 S. Ct. at 949–50.

34. *Id.* at 949.

35. *See id.*

36. *Id.* at 949–50 (relying on Olmstead v. United States, 277 U.S. 438 (1928)).

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

38. *Jones*, 132 S. Ct. at 950.

Relying on *Katz*, the Government argued that Jones had no reasonable expectation of privacy while traveling on public roadways.[39] Justice Scalia rejected this argument as out of hand, however, explaining that the issue before the Court is most readily addressed by the trespass approach, which *Katz* did not repudiate nor did it narrow the reach of the Fourth Amendment.[40]

Next, the Government posited that two Supreme Court decisions discussing electronic tracking devices favored its argument that the GPS surveillance of Jones did not constitute a Fourth Amendment search.[41] First, in *United States v. Knotts*,[42] the Court addressed the use of a beeper placed within some containers loaded onto a car that monitored the car's movements on public roads and tracked it to the ultimate destination where the containers were unloaded.[43] Justice Scalia explained that *Knotts* was distinguishable from *Jones* because *Knotts* applied the reasonable expectation of privacy test from *Katz*, whereas *Jones* applied the common law trespass approach.[44]

Next, the Court considered *United States v. Karo*,[45] the second beeper decision put forth by the Government.[46] Justice Scalia first noted that *Knotts* did not address "whether the installation of a beeper in a container amounted to a search or seizure" when the device was installed prior to the defendant's receipt of the container holding the device.[47] Again, Justice Scalia rejected the applicability of *Karo* because, as opposed to the defendant in *Jones*, Karo had accepted the container that contained the surveillance device, and Jones was entirely unaware that the police had placed the device on a vehicle that he already possessed.[48]

In an opinion concurring in the judgment (joined by Justices Ginsburg, Breyer, and Kagan), Justice Alito criticized Justice Scalia's trespass approach as outdated in the 21st century.[49] Instead of the trespass test utilized by the majority, Justice Alito emphasized the notion of privacy as enunciated in *Katz* and its progeny.[50] In addition to rejecting the trespass approach, Justice Alito asserted that the majority ignored the greater significance of the Government's use of long-term electronic surveillance, which can pose a much greater danger of breaches of privacy than the trespassory nature of the attachment of the device.[51] Moreover, the concurrence argued that

39. *Id.*
40. *Id.* at 950–51.
41. *Id.* at 950–53.
42. United States v. Knotts, 460 U.S. 276 (1983).
43. *Jones*, 132 S. Ct. at 951–52 (citing *Knotts*, 460 U.S. at 278, 280–81).
44. *Id.* at 952 (discussing *Knotts*, 460 U.S. at 278).
45. United States v. Karo, 468 U.S. 705 (1984).
46. *Jones*, 132 S. Ct. at 952.
47. *Id.* (discussing *Karo*, 468 U.S. at 713).
48. *Id.* (discussing *Karo*, 468 U.S. at 712).
49. *Id.* at 957–58 (Alito, J., concurring).
50. *Id.* at 959–61.
51. *Id.* at 961.

differences in the timing of the physical trespass or how the surveillance occurs might cause inconsistent results.[52] Next, Justice Alito posited that the majority's approach would lead to different results depending on the property law in a given state or how the common law has developed in that jurisdiction.[53] Lastly, Justice Alito determined that, as technology develops and evolves, the government may use electronic surveillance to track suspects without any necessity to trespass.[54] Ultimately, he concluded that the reasonable expectation of privacy standard warranted a suppression of the evidence in Jones's trial because of the excessive length and pervasiveness of the GPS surveillance.[55]

Finally, Justice Sotomayor issued a decision concurring with the majority decision because she believed the Government had physically intruded into Jones's vehicle, which had constitutional protections.[56] She acknowledged, however, that both tests were viable depending on the factual circumstances, but that GPS surveillance poses other concerns based on the amount of information that law enforcement can gather efficiently and easily.[57] She posited that knowledge that the government is engaged in such pervasive surveillance may cause individuals to forgo First Amendment associational and expressive rights.[58] Most significantly, Justice Sotomayor called for reconsideration of the third-party doctrine, which prevents individuals from asserting a privacy right when they share their information or data.[59]

II. *RILEY V. CALIFORNIA*

David Riley encountered police officers during a routine traffic stop, which led to an arrest for the possession of two concealed firearms that were stashed under the hood.[60] In addition to searching Riley during his arrest, the police officers took his smart phone and searched through it, discovering text messages that purportedly linked him to gang activity.[61] A couple of hours later at the police station, with Riley under arrest, a police detective searched through his cell phone looking for evidence of criminal activity that eventually led to evidence of Riley's purported involvement in an earlier,

52. *Id.*
53. *Id.* at 961–62.
54. *Id.* at 962.
55. *Id.* at 962–64.
56. *Id.* at 954 (Sotomayor, J., concurring).
57. *Id.* at 954–55.
58. *Id.* at 956.
59. *Id.* at 957; *see also* Smith v. Maryland, 442 U.S. 735, 742 (1979) (rejecting an expectation of privacy for numbers dialed on a cell phone); United States v. Miller, 425 U.S. 435, 443 (1976) (stating that the Fourth Amendment does not protect information revealed to a third party).
60. Riley v. California, 134 S. Ct. 2473, 2480 (2014); *see also* Owsley, *TriggerFish*, *supra* note 7, at 225–26 (addressing *Riley*).
61. *Riley*, 134 S. Ct. at 2480.

gang-related shooting.[62] Based on this search, the Government charged Riley with attempted murder, assault with a firearm, and firing at an occupied vehicle.[63]

Before trial, Riley moved to suppress the evidence gathered from the warrantless search of his cell phone, arguing that the search violated the Fourth Amendment and that there were no exigent circumstances justifying the search.[64] After the trial court denied Riley's motion to suppress, the jury convicted him based in large part on the evidence obtained from his cell phone, resulting in his sentence of fifteen years to life in prison.[65]

On February 13, 2013, the California Court of Appeals affirmed Riley's conviction, and the California Supreme Court subsequently denied his petition for review.[66] The Supreme Court granted Riley's petition for a writ of certiorari.[67]

In a companion case, police officers arrested Brima Wurie after allegedly witnessing him engage in narcotics trafficking.[68] During the arrest, officers seized two cell phones from Wurie, and later at the police station officers examined them, discovering that Wurie's flip phone was receiving calls from a phone number labeled "my house."[69] The officers then opened the flip phone, first viewing a picture of a woman with a baby, then locating the actual number associated with "my house," which they subsequently traced to an apartment building.[70]

Next, the officers went to the address and saw Wurie's name on a mailbox as well as a woman who looked like the picture in the flip phone.[71] They then obtained a search warrant for his apartment, and the subsequent search resulted in finding marijuana, crack cocaine, and weapons that in turn led to federal charges for possession and distribution of crack cocaine as well as being a felon in possession of a firearm.[72]

Wurie filed a motion to suppress the evidence from the search of his apartment, asserting that the search was based on an unconstitutional search of his cell phone.[73] The United States District Court for the District of

62. *Id.* at 2480–81.
63. *Id.* at 2481.
64. *Id.*
65. *Id.*
66. *Id.*
67. Riley v. California, 134 S. Ct. 999, 999 (2014).
68. *Riley*, 134 S. Ct. at 2481; *see also* Owsley, *TriggerFish*, *supra* note 7, at 226 (discussing *Wurie*).
69. *Riley*, 134 S. Ct. at 2481.
70. *Id.*
71. *Id.*
72. *Id.* at 2481–82.
73. *Id.* at 2482.

Massachusetts denied his motion.[74] Consequently, the court convicted Wurie of the three charges and he received a sentence of 262 months in prison.[75]

Wurie appealed his conviction to the United States Court of Appeals for the First Circuit, which vacated his convictions based on the court's reversal of the denial of his motion to suppress.[76] That court concluded that because cell phones are unique (they contain so much personal information and typically do not pose any threat to officer safety), they may not be searched after an arrest without a search warrant.[77] The Federal Government filed a petition for a writ of certiorari, which the Supreme Court granted.[78]

In an opinion by Chief Justice Roberts, which all the other members of the Court joined (except Justice Alito, who wrote a separate opinion concurring in the judgment and dissenting in part), the Court began its analysis by discussing the Fourth Amendment's reasonableness requirement.[79] This reasonableness requirement also applies to searches subsequent to arrest.[80]

In light of the Court's prior decisions in *Chimel v. California*, *United States v. Robinson*, and *Arizona v. Gant*, the Court analyzed what protections the Fourth Amendment provided to the cell phones possessed by both Riley and Wurie.[81] First, Chief Justice Roberts declined to extend the protections enunciated in *Robinson* because they are inapplicable to searches of all the information available on cell phones.[82] Next, the Court applied the *Chimel* factors to searches of cell phones incident to arrests.[83] First, the Court explained that the personal information stored in a cell phone cannot be used as a weapon to injure any police officers.[84] Next, the Court discussed the *Chimel* factor focusing on preventing arrestees from destroying evidence of any criminal activity and concluded that, notwithstanding some unique features about cell phones as opposed to other types of evidence that can be destroyed during an arrest, the Government's concern was overblown.[85] The arrest of a subject suspected of criminal activity does not entirely suspend the

---

74. United States v. Wurie, 612 F. Supp. 2d 104, 111 (D. Mass. 2009), *rev'd and remanded*, 728 F.3d 1 (1st Cir. 2013); *see also* Charles E. MacLean, *But Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41, 61–62 (2012) (criticizing the district court's decision in *Wurie*).

75. *Riley*, 134 S. Ct. at 2482.

76. *Wurie*, 728 F.3d at 14.

77. *Id.*; *accord Riley*, 134 S. Ct. at 2482.

78. United States v. Wurie, 134 S. Ct. 999, 999 (2014).

79. *Riley*, 134 S. Ct. at 2482; *see also* Owsley, *TriggerFish*, *supra* note 7, at 226–27 (discussing *Riley*).

80. *Riley*, 134 S. Ct. at 2482–84 (discussing Arizona v. Gant, 556 U.S. 332 (2009); United States v. Robinson, 414 U.S. 218 (1973); and Chimel v. California, 395 U.S. 752 (1969)).

81. *Id.* at 2484.

82. *Id.* at 2484–85.

83. *Id.* at 2484–86.

84. *Id.* at 2485–86.

85. *Id.* at 2486–87.

individual's Fourth Amendment rights.[86] Given the storage capability of today's cell phones, which Chief Justice Roberts characterized as minicomputers, cell phones have large amounts of private personal data such that they are different in both quantity as well as quality of the records.[87]

Besides pushing for an extension of the *Robinson* standard, both California and the United States suggested a number of alternatives in which warrantless cell phone searches should be permitted.[88] For example, the United States proposed a standard, based on *Gant*, allowing police officers to search an arrestee's cell phone without a warrant when it is reasonable to believe that the cell phone would contain evidence related to the crime for which the person was arrested.[89] The Court rejected this suggestion in part because *Gant* was based on specific circumstances related to vehicles and an arrest that were not present in the cell phone context.[90] Next, the United States suggested a rule in which an officer could search a cell phone if the officer reasonably believes that it would reveal evidence relevant to the crime, the arrestee's identity, or information concerning the officer's safety, but the Court rejected this rule as too broad.[91] Finally, the Court rejected a rule that would enable officers to search cell phone logs based on *Smith v. Maryland*, in which the Court ruled that one does not have a reasonable expectation of privacy in the telephone numbers that one calls.[92] The Court concluded, however, that this approach ignored the fact that examination of Wurie's cell log constituted a search as well as the fact that call logs can contain much more information than simply a list of numbers called.[93]

California suggested that the rule allows warrantless searches if the information obtained could have been obtained in a pre-digital world, such as a photo in a wallet as opposed to one in a cell phone.[94] Nonetheless, the Court rejected this analogue as overly broad because a cell phone could hold thousands of photos or years of bank records.[95]

In conclusion, the Court was cautious to ensure that its decision would not be interpreted to bar cell phone searches entirely when the phone is seized

---

86. *Id.* at 2488–89.

87. *Id.* at 2489–91; *see also* MacLean, *supra* note 74, at 61 ("Cell phones are more like extensive computers than wallets.").

88. *Riley*, 134 S. Ct. at 2491–94.

89. *Id.* at 2492.

90. *Id.* (discussing Arizona v. Gant, 556 U.S. 332, 343, 345 (2009)).

91. *Id.*

92. *Id.*; *see* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

93. *Riley*, 134 S. Ct. at 2492–93.

94. *Id.* at 2493; *see also* United States v. Park, No. CR-05-375-SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) ("[M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.").

95. *Riley*, 134 S. Ct. at 2493; *see also* MacLean, *supra* note 74, at 62 (dismissing any analogy because "[a] cell phone can hold millions of pages of data, while a wallet may hold a few").

as part of an arrest.[96] Even though the general exception authorizes a search of a cell phone incident to arrest, the Court (as well as the defendants) acknowledged that exceptions may be available in some of the extreme circumstances raised in briefs and during oral argument.[97] In other words, *Riley* heralds a new era in Fourth Amendment jurisprudence, in which the protection of valuable papers has moved from the home and into the cell phone in one's pocket.[98] This transition only stands to reason in light of the overwhelming significance that cell phones have taken on in most people's lives, as well as the large amount of personal information they typically contain.[99]

Even in his concurring opinion, Justice Alito agreed with the result insofar as the majority's approach called for a reassessment of how privacy interests should be balanced in light of law enforcement's interest in investigating criminal activity.[100] Justice Alito, however, also expressed a preference that state and federal legislatures address this balance as opposed to leaving it to the courts.[101]

III. THE SUPREME COURT'S DEVELOPMENT OF THE THIRD-PARTY DOCTRINE

Although the majority in *Jones* based its decision on a trespass theory of the Fourth Amendment, the decision as a whole can be read to support an approach in which individuals' privacy rights in their cell phones' locational data receives the Court's reinvigorated protection based on the Fourth Amendment.[102] In *Riley*, the Court bolstered this approach when it ensured that there are protections for the vast amount of data available on a cell phone, including locational data.[103]

The issue with using a cell phone's GPS capability to track the phone's user is that, unlike in *Jones*, there is no trespass of the user's cell phone.[104] Instead, the investigating law enforcement agents would simply contact the cell phone provider because the cell phone manufacturer includes GPS

---

96. *Riley*, 134 S. Ct. at 2493; *see* United States v. Phillips, 9 F. Supp. 3d 1130, 1140 (E.D. Cal. 2014); United States v. Dixon, 984 F. Supp. 2d. 1347, 1350 (N.D. Ga. 2013).

97. *Riley*, 134 S. Ct. at 2494.

98. *See* Adam Lamparello & Charles MacLean, Riley v. California*: The New* Katz *or* Chimel*?*, 21 RICH. J.L. & TECH., no. 1, 2014, at 15; *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 18 (2004) ("Electronic surveillance is 'indiscriminate' in the sense that it may obtain information that has no link to criminal activity. Any number of entirely innocent people may either call or be called from a wiretapped phone. Electronic surveillance casts a far wider net than a traditional search for evidence of a crime at a target's home or business.").

99. *See Riley*, 134 S. Ct. at 2490.

100. *Id.* at 2496–97 (Alito, J., concurring).

101. *Id.* at 2497–98.

102. *See* Owsley, *Cell Tower Dumps*, *supra* note 7, at 36.

103. *See Riley*, 134 S. Ct. at 2490–91 (majority opinion).

104. *See* United States v. Skinner, 690 F.3d 772, 779–80 (6th Cir. 2012).

technology on the device when the customer purchases it.[105] If the third-party doctrine applies to this data, then the user arguably has no protection against any warrantless search.[106]

To address the third-party doctrine, one must first consider the Fourth Amendment. That amendment mandates:

> 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[107]

Courts have determined cell phones to be effects within the meaning of the Fourth Amendment.[108] The general theory is that if a person voluntarily provides access to that individual's personal information, then there is no reasonable expectation of privacy and thus, no protection pursuant to the Fourth Amendment.[109] The two leading cases espousing this view are *United States v. Miller* and *Smith v. Maryland*.[110]

A. United States v. Miller

The third-party doctrine serves as the greatest impediment to a de facto announcement that warrants are necessary any time the government seeks to use a cell phone as a tracking device. The Supreme Court enunciated the third-party doctrine for the first time in *Miller*.[111] Mitchell Miller was essentially in the moonshine business in Georgia and had some bad luck in that a deputy sheriff pulled over two of his business partners with distillery equipment and ingredients in their van.[112] Then, a few weeks later, a fire at the warehouse that Miller rented led to the discovery of a very large distillery

---

105. *See id.* at 781 ("[T]he Government never had physical contact with Skinner's cell phone; he obtained it, GPS technology and all, and could not object to its presence.").

106. *See id.* at 780 (distinguishing *Jones* because the defendant's cell "phone included the GPS technology used to track the phone's whereabouts"); *see also* Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207, 232 (2013) (discussing *Skinner* in comparison to *Jones*).

107. U.S. CONST. amend. IV.

108. *See, e.g.*, *In re* Application for Tel. Info. Needed for a Criminal Investigation, No. 15-XR-90304-HRL-1(LHK), 2015 WL 4594558, at *6 (N.D. Cal. July 29, 2015) (citing Oliver v. United States, 466 U.S. 170, 177 n.7 (1984)); United States v. Aispuro, No. 13-10036-01-MLB, 2013 WL 3820017, at *14 (D. Kan. July 24, 2013) (citing United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)); *accord* Tracey v. State, 152 So. 3d 504, 524 (Fla. 2014).

109. *See, e.g.*, *Aispuro*, 2013 WL 3820017, at *8 (explaining that officers may conduct warrantless vehicle searches if the person in control of the vehicle voluntarily consents).

110. Smith v. Maryland, 442 U.S. 735, 742–43 (1979); United States v. Miller, 425 U.S. 435, 440–41 (1976).

111. *See Miller*, 425 U.S. at 440–41.

112. *Id.* at 437.

and 175 gallons of bootleg whiskey.[113] Based on these discoveries, ATF agents served subpoenas—issued by the Office of the United States Attorney—on the presidents of two banks where Miller had accounts, ordering them to produce all records related to his accounts.[114] The prosecution, at trial, introduced copies of checks obtained from these banks to establish the overt acts charged in the conspiracy.[115]

In a motion to suppress, Miller argued that the subpoenas were defective because a judge did not issue them, so the court should have excluded the bank records.[116] The district court denied the motion to suppress, but the appellate court reversed, finding that the district court's holding violated Miller's Fourth Amendment rights.[117]

Writing for the majority, Justice Powell held that Miller did not have a Fourth Amendment interest in his bank records.[118] Specifically, the Court found that no reasonable expectation of privacy existed in bank records that Miller freely provided to the banks, and that he took the risk in conveying his information to bank officials.[119]

B. Smith v. Maryland

In *Smith*, the Supreme Court extended the third-party doctrine to a case involving a pen register.[120] After a woman was robbed, she gave the police a description of the robber and the 1975 dark green and tan Monte Carlo that she noticed him working on near the crime scene.[121] Shortly after the robbery, the victim began receiving obscene telephone calls from a man who identified himself as her robber.[122] Around this same time, the 1975 Monte Carlo was seen again, and the license plate number recorded led to the identification of Michael Smith.[123] The police then requested that the telephone company install a pen register on Smith's residence to record his outgoing dialed telephone numbers, which revealed that he had been calling the woman.[124]

In part based on this evidence, Smith was indicted for robbery.[125] He filed a motion to suppress the evidence related to the pen register because the police had failed to obtain a warrant before the telephone company installed

113. *Id.*
114. *Id.* at 437–38.
115. *Id.* at 438.
116. *Id.* at 438–39.
117. *Id.* at 437.
118. *Id.* at 440.
119. *Id.* at 442–43.
120. Smith v. Maryland, 442 U.S. 735, 742 (1979).
121. *Id.* at 737; Smith v. State, 389 A.2d 858, 859 (Md. 1978).
122. *Smith*, 442 U.S. at 737; *Smith*, 389 A.2d at 859.
123. *Smith*, 442 U.S. at 737; *Smith*, 389 A.2d at 859.
124. *Smith*, 442 U.S. at 737; *Smith*, 389 A.2d at 859–60.
125. *Smith*, 442 U.S. at 737; *Smith*, 389 A.2d at 859–60.

it.[126] After denial of his motion and conviction, Smith appealed, and the Maryland Court of Appeals addressed whether the evidence from the pen register was properly admitted at his trial.[127] That court, however, eventually affirmed Smith's conviction.[128]

Justice Blackmun began the Court's analysis by discussing *Katz*.[129] Specifically, he addressed whether installation and use of a pen register to obtain Smith's dialed telephone numbers constituted a Fourth Amendment search.[130] He noted that Smith's argument had to rest on a position that he had a reasonable expectation of privacy in the telephone numbers that he dialed.[131] Justice Blackmun further explained that all telephone customers are aware that they are providing the telephone company with information about the numbers that they dial and, as such, do not have a reasonable expectation of privacy in those numbers.[132] Moreover, even if a customer, such as Smith, had some expectation of privacy, it would not be a reasonable one.[133] The Court invoked and analyzed *Miller*, noting that just like depositors assume the risk in providing the bank their information, so too does the telephone user.[134] Consequently, the installation of the pen register was not a Fourth Amendment search requiring a warrant.[135]

IV. CONGRESSIONAL ACTION HAS LIMITED THE THIRD-PARTY DOCTRINE AS IT RELATES TO CELL PHONES AS TRACKING DEVICES

One notices in reading and considering both *Miller* and *Smith* that the Court is dated in its approach to the technology and the disclosures made to third parties.[136] In *Miller*, the disclosure was premised on exchanging personal financial information with a bank teller.[137] Today, few people have such interactions with a real person, but instead do most banking online or by ATM.[138] Similarly, in *Smith*, the defendant was using a landline telephone with technology much different than that used today.[139] These developments

126. *Smith*, 442 U.S. at 738; *Smith*, 389 A.2d at 860.
127. *Smith*, 442 U.S. at 738.
128. *Id.*
129. *Id.* at 739.
130. *See id.* at 741.
131. *Id.* at 742.
132. *Id.*
133. *Id.* at 743.
134. *Id.* at 743–44 (discussing United States v. Miller, 425 U.S. 435, 442–44 (1976)).
135. *Id.* at 745–46.
136. *See, e.g.*, *id.* at 737, 743 (addressing Fourth Amendment protection for the use of home phones).
137. *Miller*, 425 U.S. at 442.
138. *See generally* Christian N. Watson, *The Growth of Internet-Only Banks: Brick and Mortar Branches Are Feeling the "Byte"*, 4 N.C. BANKING INST. 345 (2000) (discussing the growth and impact of online-only banks).
139. *Smith*, 442 U.S. at 737, 743. *See generally* LEE RAINIE, INTERNET, BROADBAND, AND CELL PHONE STATISTICS, PEW RES. CTR. (Jan. 5, 2010), http://www.pewinternet.org/files/old-media/Files/

greatly limit the ability of bank or cell phone customers to avoid providing all manners of information, even though an actual third person is typically not involved.[140]

In addition to the changes in technology that impact the third-party doctrine, Congress has not been entirely silent regarding cell phone location information.[141] Two federal statutes explicitly discuss location information, and these statutes support the position that Congress has sought to protect this information.[142] As an initial matter, there is also a federal statute that deals with tracking devices and informs the discussion about cell phone location data.[143]

A. Federal Tracking Device Statute

In his *Riley* concurrence, Justice Alito suggested that a legislative solution would be preferable, notwithstanding the lack of any developments regarding electronic surveillance in recent years.[144] In 1986, in the Electronic Communications Privacy Act (ECPA),[145] Congress enacted legislation authorizing mobile tracking devices: "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."[146] Consistent with the Federal Rules of Criminal Procedure, judges may issue search warrants for tracking devices.[147]

Congress defined a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[148] This federal statute directly addresses the question of whether cell phones can be used as a tracking device.[149] Based on the statutory definition, cell phones should be construed as tracking devices.[150] However, one

---

Reports/2010/PIP_December09_update.pdf (reporting various statistics about modern cell phone and internet usage).

140. *See generally, e.g.*, OFFICE OF TECH. ASSESSMENT, NO. 293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (Oct. 1985), http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/15/fgit-1985.pdf (providing research of technological advancement in telephone use and suggestions for congressional legislation).

141. *See, e.g.*, 18 U.S.C. § 2701 (2012).

142. *See infra* Part IV.B–C.

143. *See infra* Part IV.A.

144. *See* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014); *see also* Owsley, *Cell Tower Dumps*, *supra* note 7, at 42–43 (discussing the difficulties of relying on Congress to enact new legislation to address new electronic surveillance technology).

145. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

146. 18 U.S.C. § 3117(a) (2012); 100 Stat. 1858.

147. FED. R. CRIM. P. 41(e)(2)(C).

148. 18 U.S.C. § 3117(b); *see also* FED. R. CRIM. P. 41(a)(2)(E) (incorporating the definition in § 3117(b) for purposes of the rule addressing search warrants).

149. 18 U.S.C. § 3117.

150. *See id.*

commentator has asserted that if the legislative history is considered, then arguably, cell phones are not tracking devices.[151]

Several federal district courts have addressed the applicability of § 3117 to the use of cell phones as tracking devices with differing results. For example, one Maryland court, applying ECPA, held that the government could track in real time a targeted cell phone provided that the tracking was not done in private places.[152] Similarly, a federal court in New York concluded that obtaining a cell phone's geolocation data pursuant to the Stored Communications Act did not convert the cell phone into a tracking device pursuant to § 3117.[153] These decisions tend to ignore the straightforward nature of the federal definition for a tracking device.[154]

On the other hand, a Texas federal court concluded that the ability of the government to obtain a cell phone user's present location based on analysis of the cell phone's real time cell site data constituted a tracking device and thus required a demonstration of probable cause before a judge could issue an order authorizing the tracking.[155] Similarly, a New York federal court ruled that a governmental request for a pen register to obtain real-time location information was a tracking device that required a showing of probable cause.[156]

The use of the word *installation* in § 3117(a) is not determinative of whether the tracking device must actually be installed for it to satisfy the definition.[157] That subsection is focusing on territorial authority, whereas § 3117(b) focuses on the definition.[158] Indeed, installation could be done not just manually with a physical intrusion but also electronically.[159] As the Supreme Court explained in *Riley*, cell phones have a myriad of uses and capabilities, including "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[160] A

151. M. Wesley Clark, *Cell Phones As Tracking Devices*, 41 VAL. U. L. REV. 1413, 1472–73 (2007).

152. *In re* Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification Sys. on Tel. Nos. [Sealed] and [Sealed] and the Prod. of Real time Cell Site Info., 402 F. Supp. 2d 597, 603–05 (D. Md. 2005).

153. *See generally In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129 (E.D.N.Y. 2013) (concluding that a cell phone's geolocation data does not equate to a tracking device).

154. *See supra* text accompanying note 148.

155. *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005).

156. *In* re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 326–27 (E.D.N.Y. 2005).

157. United States v. White, 62 F. Supp. 3d 614, 624–25 (E.D. Mich. 2014).

158. *Id.* at 625.

159. *In re* Application of U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 898 (S.D. Tex. 2014) ("[A]n 'installation' in our digital age need not entail a physical process, like placing a beeper under a truck bumper; as often as not the term refers to a screen tap or keystroke by which new software is electronically 'installed' on digital devices."); *accord White*, 62 F. Supp. 3d at 614.

160. Riley v. California, 134 S. Ct. 2473, 2489 (2014); *accord In re Application of U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F. Supp. 3d at 898.

tracking device also fits on this list, especially given the existing, explicit geolocation features already on many smart phones.[161]

B. Wireless Communications and Public Safety Act

In the Wireless Communications and Public Safety Act of 1999, Congress specifically addressed cell phone location information and data.[162] This Act, which amended the Communications Act of 1934 and the Telecommunications Act of 1996, sought to upgrade 911 emergency services for cell phones around the country.[163] In the Telecommunications Act, Congress included a definition of "customer proprietary network information" to mean "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier–customer relationship."[164]

In amending these statutes, Congress explained that a cell phone user's information is private, notwithstanding the fact that the telecommunications provider has access to it:

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to *individually identifiable customer proprietary network information* in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[165]

Moreover, unless the subscriber has expressly authorized the use, "a customer shall not be considered to have approved the use or disclosure of or

---

161. *See supra* text accompanying notes 6–16.

162. *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified as amended in scattered sections of 47 U.S.C.).

163. *Id.* § 2; *see also* 47 U.S.C. § 251(e)(3) (2012) (requiring 9-1-1 as the universal emergency phone number for cell phones); Nuvio Corp. v. FCC, 473 F.3d 302, 311 (D.C. Cir. 2006) (discussing the Wireless Communications and Public Safety Act); *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 841–42 (S.D. Tex. 2010) (discussing the Wireless Communications and Public Safety Act), *vacated*, 724 F.3d 600 (5th Cir. 2013).

164. Telecommunications Act of 1996, Pub. L. No. 104-104, § 702, 110 Stat. 56, 149 (1996) (codified at 47 U.S.C. § 222(h)(1)); *see also* 47 U.S.C. § 251(f)(1)(A) (noting the possibility of an exemption for rural telephone companies).

165. 47 U.S.C. § 222(c)(1) (emphasis added); *see also* Tank v. T-Mobile USA, Inc., No. 1:12-cv-10261, 2014 WL 4121134, at *2–3 (N.D. Ill. Aug. 20, 2014) (noting the limited scope of access to CPNI). *But see In re* Application of U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 6:08-6038M-REW, 2009 WL 8231744, at *9 n.17 (E.D. Ky. Apr. 17, 2009) ("The privacy afforded by this section is statutory, not constitutional, and exists in recognition of other law regulating disclosure.").

access to" the subscriber's "call location information."[166] In enacting the statute, Congress explicitly included location information within the definition of "customer proprietary network information."[167] As a general rule, the customer, as opposed to the provider, determines the level of privacy that should be maintained.[168] Of course, there are exceptions that allow the provider to use the customer's personal information, including for billing and safety purposes.[169] Nonetheless, § 222(f)(1) recognizes congressional concern about the sensitive nature of the subscriber information that the provider collects to operate its telecommunications system and congressional desire to ensure that this information is afforded a very high level of protection.[170]

The legislative history of the Wireless Communications and Public Safety Act reveals that members of Congress were deeply concerned about the statute's privacy protections.[171] In proposing a privacy amendment to the bill, Representative Edward Markey voiced his belief that the statute could "pose significant risks for compromising personal privacy."[172] He elaborated on his apprehensions, explaining:

> [Cell phone] technology also avails wireless companies of the ability to locate and track individual's movements throughout society, where you go for your lunch break; where you drive on the weekends; the places you visit during the course of a week is your business. It is your private business, not information that wireless companies ought to collect, monitor, disclose, or use without one's approval.[173]

Representative Markey's statement foretold similar ones raised in judicial opinions, including Justice Sotomayor's concurring opinion in *Jones*: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political,

---

166. 47 U.S.C. § 222(f)(1); *see also In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 841–42 (explaining that telecommunications providers must "protect the confidentiality of 'customer proprietary network information' (CPNI), that is, information about a customer's use of the service that was made available to the carrier by the customer solely by virtue of the carrier–customer relationship").

167. 47 U.S.C. § 222(h)(1)(A) ("The term 'customer proprietary network information' means information that relates to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." (emphasis added)).

168. *See id.*

169. *See id.* § 222(d).

170. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999); *see also In re* Application for Pen Register & Trap/Trace Device With Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) (explaining that "location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer").

171. 145 CONG. REC. 24,989 (1999).

172. *Id.*

173. *Id.*

professional, religious, and sexual associations."[174] Finally, Representative Markey indicated that the telecommunications providers should not be allowed to sell customer information without customer approval in part because "[w]herever your cell phone goes becomes a monitor of all of your activities."[175]

Other representatives voiced worries about cell phone subscribers' privacy. Congressman Thomas Bliley explained that "[i]t is not appropriate to let government or commercial parties collect such information or keep tabs on the exact location of individual subscribers."[176] Consequently, the proposed legislation would "ensure that such call location information is not disclosed without the authorization of the user, except in emergency situations, and only to specific personnel."[177] In discussing Representative Markey's privacy amendment, Congressman Gene Green expressed appreciation because "we do not want Big Brother looking over our shoulders," notwithstanding the statute's safety goals.[178] Representative Wilburt Tauzin echoed these sentiments, stating that the privacy amendment "protects us from Government knowing where you are going and what you are doing in your life."[179]

Some courts have started to reject the application of *Smith* and *Miller* to CSLI, in part, based on analysis of the Wireless Communications and Public Safety Act.[180] The United States Court of Appeals for the Fifth Circuit rejected this argument without much analysis.[181] More recently, however, the Fifth Circuit acknowledged that the Supreme Court's decision in *Riley*

---

174. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *see also* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."(footnote omitted)); People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) (stating that GPS data will reveal "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").

175. 145 CONG. REC. 24,989.

176. *Id.* at 24,992.

177. *Id.*

178. *Id.* at 24,991.

179. *Id.* at 24,989.

180. *See, e.g.*, *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 841–45 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

181. *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 608 n.10.

may call *Historical Cell Site Data* into question.[182] Moreover, the specific language in the Act should overcome the Stored Communications Act's general language.[183]

Additionally, another court held § 222(a) requires telecommunications providers to protect their location information.[184] In *United States v. White*, the federal district court determined that when an individual uses a cell phone, that person is not consenting to the dissemination of his or her call location information.[185] Moreover, the court further explained, cell phone subscribers "reasonably may expect their providers to comply with the law."[186] Ultimately, this statute manifests congressional intent to safeguard cell phone subscriber's location information.[187]

C. Communications Assistance for Law Enforcement Act

In the Communications Assistance for Law Enforcement Act of 1994,[188] Congress addressed "law enforcement's perceived need for assistance in coping with new communications technology."[189] Specifically, Congress sought to enhance law enforcement's ability to engage in electronic surveillance by mandating that telecommunications providers and telecommunications equipment manufacturers ensure that the services and equipment enabled this surveillance.[190] Moreover, the statute's legislative history explained that its purpose was "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services."[191] As one commentator explained, the Communications Assistance for Law Enforcement Act was designed to enable law

182. United States v. Guerrero, 768 F.3d 351, 360 (5th Cir. 2014) (discussing the *Riley* approach to different technologies and its potential impact on future cases); *see also* Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 291–92 (2015) (noting that *Guerrero* acknowledged that the Supreme Court may ultimately reconsider *Smith v. Maryland* and its third-party doctrine as applied to CSLI).

183. *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 675 n.2 (S.D. Tex. 2015).

184. United States v. White, 62 F. Supp. 3d 614, 623 (E.D. Mich. 2014).

185. *Id.*

186. *Id.*

187. *Id.*

188. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 47 U.S.C.).

189. Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 1002 (2008).

190. *Id.* at 1002–03; Owsley, *TriggerFish*, *supra* note 7, at 196.

191. H.R. REP. NO. 103-827, at 9 (1994).

enforcement to adapt to new telecommunications technologies in regards to its electronic surveillance.[192]

Nonetheless, Congress specifically banned law enforcement from obtaining a cell phone's location pursuant to a pen register application: "[I]nformation acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the *physical location* of the subscriber."[193] This ban on location information applied to both the telecommunications companies that would provide it as well as law enforcement agencies that would obtain it.[194] Indeed, then-FBI Director Louis Freeh testified that the legislative proposal before Congress would not alter the landscape regarding legal authority for pen registers.[195] Regarding the use of pen registers to obtain location information of the cell phone user, Director Freeh attempted to allay such concerns:

> Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. Even when such generalized location information, or any other type of "transactional" information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.
>
> In order to make clear that the acquisition of such information is not being sought through the use of a pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: "* * *, except that such information [call setup information] shall not include any information that may disclose the physical location of a mobile

192. Clark, *supra* note 151, at 1423.

193. 47 U.S.C. § 1002(a)(2)(B) (1998) (emphasis added).

194. *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 307 n.9 (E.D.N.Y. 2005); Owsley, *TriggerFish*, *supra* note 7, at 196.

195. *See Police Access to Advanced Communication Systems: Hearing Before the Subcomm. on Tech. & the Law of the Comm. on the Judiciary, U.S.S., and the Subcomm. on Civil & Constitutional Rights of the Comm. on the Judiciary, H.R.*, 103d Cong. 33 (1994) [hereinafter *Hearing*] (statement of Louis J. Freeh, Director, FBI), 1994 WL 223962; *see also In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 955 (E.D. Wis. 2006) (discussing Director Freeh's testimony); *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d 211, 216–17 (W.D.N.Y. 2006) (same); Casey, *supra* note 189, at 1003 (same); Owsley, *TriggerFish*, *supra* note 7, at 196 (same). One commentator, however, has argued that the bar against disclosing a subscriber's physical location should not be construed as a restriction on law enforcement obtaining real-time cell phone location data. Clark, *supra* note 151, at 1464.

> facility or service beyond that associated with the number's area code or exchange."[196]

Interestingly, he noted that using devices that track individuals requires some judicial authorization, at least if the tracking crosses into a private sphere.[197] Moreover, the federal government, through its chief law enforcement official, sought to establish that it obtained location information without a pen register.[198]

As with the Wireless Communications and Public Safety Act, the Communications Assistance for Law Enforcement Act not only contemplates the use of location tracking capabilities that cell phones have, but more importantly bars the use of this technology to track a cell phone.[199] No doubt, Congress was well aware of the third-party doctrine and its implications for Fourth Amendment protections and cell phone users' privacy interests. Nonetheless, these statutes prevent the government from obtaining location information from cell phone data.

V. CONCLUSION

Based on the third-party doctrine, cell phone subscribers arguably do not have a reasonable expectation of privacy in their cell phone's data that is transmitted and captured by telecommunications providers.[200] In other words, cell phone users should know that when they have their cell phone in close proximity, it provides their location information, which providers routinely collect and store.[201]

As an initial matter, the pen register at issue in *Smith* involved a landline in which the government sought the records of an outgoing number.[202] The pen register at issue in *Smith* is antiquated to say the least; I have routinely referred to it as my grandparents' pen register.[203] One scholar explained that technology changed, rendering a reassessment necessary:

> The third party and public exposure doctrines emerged at a time when modern surveillance capabilities were beyond imagination. Today, these previously unimaginable technologies are not merely law enforcement tools; they are essential parts of our daily lives. The GPS tracking and cell phone cases have forced courts to consider how the ongoing digital

196. *Hearing*, *supra* note 195 (citation omitted).
197. *Id.*
198. United States v. Karo, 468 U.S. 705, 713–14 (1984).
199. *See supra* text accompanying note 193.
200. *See supra* text accompanying notes 104–06.
201. *See supra* text accompanying notes 1–16.
202. Smith v. Maryland, 442 U.S. 735, 737 (1979).
203. United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at *6 (N.D. Cal. Mar. 2, 2015) ("[T]he pen registers employed in 1979 bear little resemblance to their modern day counterparts.").

> revolution affects the reasonable expectation of privacy under the Fourth Amendment.[204]

Originally, law enforcement could not use pen registers to determine whether a communication existed.[205] Instead, pen registers "disclose[d] only the telephone numbers that ha[d] been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [was] disclosed by pen registers."[206] Just as the *Riley* Court "rejected the government's reliance on old cases holding that police could search the physical belongings of an arrestee, in order to justify searching the data on an arrestee's cell phone," reliance on *Smith*—addressing whether a cell phone user has a reasonable expectation in the information the government could obtain with a modern pen register—is misplaced.[207]

The United States Court of Appeals for the Third Circuit rejected the argument that dialing a telephone number on one's cell phone conveys information to a third party: "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. [Moreover], it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."[208] The Northern District of California recently concluded:

> *Miller* and *Smith* do not control the analysis here because the generation of historical CSLI via continually running apps or routine pinging is not a voluntary conveyance by the cell phone user in the way those cases demand. Where, as here, an individual has not voluntarily conveyed information to a third party, her expectation of privacy in that information is not defeated under the third-party doctrine.[209]

The United States Court of Appeals for the Fourth Circuit recently held that when law enforcement officers obtain and view a cell phone's historical CSLI for a period of at least fourteen days, such examination constitutes a search that must be conducted consistent with the Fourth Amendment.[210] The

---

204. Spencer, *supra* note 182, at 301.

205. *Smith*, 442 U.S. at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

206. *Id.* (quoting *N.Y. Tel. Co.*, 434 U.S. at 167).

207. *Cooper*, 2015 WL 881578, at *6.

208. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010); *see also In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539 n.6 (D. Md. 2011) ("[H]ere the government seeks information—essentially, continuous pinging—that is not collected as a necessary part of cellular phone service, nor generated by the customer in placing or receiving a call. Under this circumstance it is difficult to understand how the user 'voluntarily' exposed such information to a third party.").

209. *In re* Application for Tel. Info. Needed for a Criminal Investigation, No. 15-XR-90304-HRL-1(LHK), 2015 WL 4594558, at *15 (N.D. Cal. July 29, 2015).

210. *See* United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015).

court further explained this conclusion: "Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user."[211] In reaching this conclusion, the panel explicitly rejected the applicability of the third-party doctrine enunciated in *Smith* and *Miller*.[212] Indeed, the court expressed grave doubts about the third-party doctrine's continued viability.[213] As with the Third Circuit, the Fourth Circuit rejected the notion that cell phone users voluntarily convey their location information simply by using their cell phones.[214]

In *Tracey v. State*, the Florida Supreme Court explained:

> Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes.[215]

In other words, as with the Third and Fourth Circuits, the court questioned the notion that the third-party doctrine and its principle of voluntary disclosure applies to cell phone location data.[216]

Moreover, continued reliance on *Miller* and *Smith* ignores the realities of modern technology. Very few people interact with bank tellers anymore in the age of online banking and ATMs.[217] Additionally, just about anyone who interacts in mainstream commerce must interact with the banking system.[218] Indeed, interpreting the Fourth Amendment, the Florida Supreme Court determined:

> [B]ecause cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs, is clearly a Fourth Amendment violation.[219]

---

211. *Id.* at 345.
212. *See id.* at 351–52.
213. *Id.* at 360.
214. *See id.* at 352–55.
215. Tracey v. State, 152 So. 3d 504, 522 (Fla. 2014).
216. *Id.*
217. *See* Sheyna Steiner, *Bank Tellers: Are They an Endangered Species?*, BANKRATE (Mar. 24, 2014), http://bankrate.com/finance/consumer-index/bank-tellers-are-they-an-endangered-species.aspx
218. *See supra* notes 138–40 and accompanying text.
219. *Tracey*, 152 So. 3d at 524; *accord In re* Application for Tel. Info. Needed for a Criminal Investigation, 15-XR-90304-HRL-1(LHK), 2015 WL 4594558, at *11 (N.D. Cal. July 29, 2015).

Moreover, Americans generally "expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings."[220]

The ubiquitous nature of cell phones in American society has become apparent even to the Supreme Court.[221] The increased sophistication of cell phone technology enables providers to accurately locate any activated cell phone.[222] People do not voluntarily provide these companies with their locations simply by using a cell phone.[223] Although courts often rely on the third-party doctrine enunciated in *Miller* and *Smith* to maintain the approach that information or data relayed by the cell phone to the provider is not protected by the Fourth Amendment, some judges have started to chip away at this approach.[224] It is time to reassess the third-party doctrine in our technological age.

220. Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 455 (2007).

221. *See* cases cited *supra* note 3.

222. *See supra* note 215 and accompanying text.

223. *See supra* note 215 and accompanying text.

224. *See supra* Part III.