Notre Dame Law Review

Volume 90
Issue 5 *Federal Courts, Practice & Procedure*

Article 10

8-2015

Whose Line Is It Anyway? Probable Cause and Historical Cell Site Data

Megan L. McKeown

WHOSE LINE IS IT ANYWAY? PROBABLE CAUSE AND HISTORICAL CELL SITE DATA

*Megan L. McKeown**

> *"For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."*
>
> —Justice Potter Stewart[1]

Introduction

In most contexts, the Supreme Court has treated warrantless searches as presumptively unreasonable under the Fourth Amendment.[2] A prosecutor can rebut this presumption by demonstrating that the search or seizure was reasonable, meaning the state bears the burden of validating the warrantless search under one of the narrowly defined warrant requirement exceptions.[3] While a warrantless search of a home is presumptively unreasonable,[4] the Fourth Amendment's protection has not been extended to require a warrant to obtain a cell phone's location information. Privacy scholars have argued considerably over what showing the government must make in order to require cell phone providers to turn over the cell phone location information data they store.[5]

During the summer of 2014, the Eleventh Circuit split with the Fifth and Third Circuits on whether the government must show probable cause to retrieve historic cell site data from cell phone providers in order to confirm that a suspect was close to where a crime was committed. The Fifth and

* J.D. Candidate, Notre Dame Law School, 2016; B.A., Communication and Political Science, Mississippi State University, 2013. This Note is dedicated to my family for encouraging me and supporting me all my life. I am grateful to Professor Patricia Bellia for her guidance and suggestions throughout the writing process and to the *Notre Dame Law Review* staff for their thoughtful edits.

1 Katz v. United States, 389 U.S. 347, 351–52 (1967) (citations omitted).

2 *See* 68 Am. Jur. 2d *Searches and Seizures* § 112 (2014).

3 *Id.*

4 *Id.*

5 *See* Cynthia Anderson, *The Privacy Debate: Does Obtaining Historic CSLI Require a Search Warrant Under the 4th Amendment?*, Legis. & Pol'y Blog (July 21, 2014), http://www.legislationandpolicy.com/1399/privacy-debate-obtaining-historic-csli-require-search-warrant-4th-amendment/.

Third Circuits have held that probable cause is not required to retrieve such information, but the Eleventh Circuit held the opposite in *United States v. Davis*.[6] Some commentators have suggested this was a questionable interpretation of the Fourth Amendment.[7] Historical cell site data is retrieved from a process whereby the cell phone communicates with the service towers nearby, and the process continues so long as the phone is powered on.[8] As the cell phone user moves away from one tower and approaches another, the phone will re-register at the closer tower.[9] Monitoring these tower switches can "map the movements of particular cell phones, and, consequently, their users."[10]

Following the decisions in the courts of appeals, a unanimous Supreme Court held in *Riley v. California*[11] that the Fourth Amendment protects the *contents* of a cell phone from seizure without probable cause.[12] But *Riley* does not adequately resolve the issue of historical cell site data retrieval because obtaining the contents of a cell phone is distinct from knowing the phone's physical locations.[13] Even though the *Riley* decision does not reconcile the

6 *See generally* United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (holding that the Fourth Amendment protects individuals from retrieval of cell phone location information), *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014); *see also In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that orders to obtain historical cell site information for specified cell phones at the points where the user places and terminates a call are not categorically unconstitutional); *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding that the Stored Communications Act does not contain any language that requires the government to show probable cause to get a court order under 18 U.S.C. § 2703(d) for cell site information).

7 *See generally* Orin Kerr, *The Eleventh Circuit's Novel Approach to the Fourth Amendment in the* Davis *Case*, VOLOKH CONSPIRACY (June 19, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/19/the-eleventh-circuits-novel-approach-to-the-fourth-amendment-in-the-davis-case/ ("The more I think about *Davis*, the more radical a reinterpretation of the Fourth Amendment it seems to be.").

8 *See* Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1747 (2009). A request from the government for historical cell site data is distinct from a request for prospective information when law enforcement wishes to obtain the information "as it happens in real time." *Id.* at 1747–48 (quoting another source) (internal quotation marks omitted). This Note will concentrate on historical, rather than real-time, cell site data, as the consensus among courts is that the government must show probable cause in order to obtain real-time information. *See id.*

9 *Id.* at 1753.

10 *Id.*

11 134 S. Ct. 2473, 2495 (2014).

12 *Id.* ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

13 *See generally* United States v. Guerrero, No. 13-50376, 2014 U.S. App. LEXIS 17584, at *16–17 (5th Cir. Sept. 11, 2014) ("Although the issues in *Riley* and in *Historical Cell Site* implicate a broader theme concerning the application of the Fourth Amendment to modern technology, they involve distinct doctrinal areas."). *Riley* did not address the constitutionality of using § 2703(d) of the Stored Communications Act to obtain historical cell site

circuit split directly, it appears at least to support the Eleventh Circuit's effort to exclude cell phone data obtained without a warrant. Notwithstanding *Riley*, the Eleventh Circuit vacated its decision in September 2014 and has decided to rehear *United States v. Davis* en banc, revealing the importance and controversial nature of this issue.[14] The Fourth Circuit will consider the same issue on appeal after the district court's decision in *United States v. Graham*,[15] in which the lower court held that information voluntarily disclosed to a third party, i.e., the cell phone company, ceases to enjoy Fourth Amendment protection. This theory of disclosure to third parties is known as the third-party doctrine.[16] The third-party doctrine takes the view that under the Fourth Amendment, an individual "assume[s] the risk" that information will be disclosed to law enforcement when a person conveys that information to the third party.[17]

While the view of the Fifth and Third Circuits is still the majority rule, it is an open question whether improvements in technology have caused the public's understanding of a reasonable expectation of privacy to evolve. Although some judges may not favor allowing the retrieval of cell phone location information without probable cause, their hands may be tied by the law as it stands, unless Congress is moved to act.

The Fourth Amendment's plain language, which protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[18] arguably does not address all technological changes, including electronic communications (as electronic communications are not "houses," "papers," or "effects"). The drafters of the Amendment could not have anticipated such advances in electronic communication. The statute at issue in the historical cell site data cases, the Stored Communications Act (SCA),[19] has made it difficult for district courts to find that probable cause is required for information retrieval in the electronic context.[20] To obtain an order, the SCA only requires that

> the governmental entity offer[ ] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or elec-

---

data from cell phone providers. *See* United States v. Mack, No. 3:13-cr-00054, 2014 U.S. Dist. LEXIS 159686, at *4 (D. Conn. Nov. 13, 2014) (noting the lack of controlling Supreme Court or Second Circuit caselaw addressing the constitutionality of § 2703(d)).

14 *See* Anderson, *supra* note 5 (noting that cell phone searches with respect to citizens' privacy rights has been a "hot topic" in the United States).

15 846 F. Supp. 2d 384 (D. Md. 2012).

16 Reihan Salam, *The Third-Party Doctrine*, NAT'L REV. ONLINE (June 12, 2013), http://www.nationalreview.com/agenda/350896/third-party-doctrine-reihan-salam.

17 *Id.* (quoting Julian Sanchez).

18 U.S. CONST. amend. IV. The Fourth Amendment continues, "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." *Id.*

19 Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012).

20 *See generally* Anderson, *supra* note 5.

> tronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[21]

The "specific and articulable facts" standard is accepted as a lower threshold than the probable cause requirement of the Fourth Amendment to obtain a warrant,[22] and challenges have been raised as to both the applicability of the statute to historical cell site location data and its constitutionality under the Fourth Amendment.[23]

Cell phones are unique in that they can offer an abundance of information about a person. As the Court recognized in *Riley*, a cell phone collects together "many distinct types of information . . . that reveal much more in combination than any isolated record," and the "phone's capacity allows even just one type of information to convey far more than previously possible."[24] All of the information that cell phones pull together can allow one's private life to be reconstructed.[25] For example, the historical information from cell phone towers can be used to locate a person's position within several feet.[26]

---

21 18 U.S.C. § 2703(d) (2012). The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act, and its constitutionality has been called into question in a few cases. The Fifth Circuit held in *In re Application of the United States for Historical Cell Site Data* (*In re Historical Cell Site Data*) that court orders under the SCA to compel cell phone providers to release historical cell site information are not per se unconstitutional. 724 F.3d 600 (5th Cir. 2013). In another case, the SCA was questioned after the government sought to retrieve the *contents* of email communications, rather than historical cell site location information. Warshak v. United States, 490 F.3d 455, 479–80 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008); *see also* United States v. Graham, 846 F. Supp. 2d 384, 405 n.16 (citing *Warshak*, 490 F.3d at 460).

22 *See In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315 (3d Cir. 2010) (holding that "the legislative history [of § 2703(d)] provides ample support for the proposition that the standard is . . . less stringent than probable cause"). An order under § 2703(d) may be issued by a federal magistrate, district court, or an equivalent state court judge, and if the issuing judge is a federal judge, the judge does not have to sit in the district in which the information is stored. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 130–31 (3d ed. 2009). The statute is silent as to whether state courts have such authority. *Id.* at 132.

23 *See* Anderson, *supra* note 5.

24 Riley v. California, 134 S. Ct. 2473, 2489–90 (2014) ("[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."); *see also* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 405 (2013) ("Much of the information stored in a person's cellular phone is deeply personal. The information can include photographs, text messages, e-mails, personal notes, records of visited websites, and many other kinds of personal information.").

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

26 *See generally* Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489 (2012); *see also* Chamberlain, *supra* note 8, at 1747 (noting that historical cell site data "can provide a relatively detailed picture of those users' geographic whereabouts"). As discussed later in

This Note argues that the "specific and articulable facts" standard does not accord with the intent of the drafters of the Fourth Amendment to protect individuals' reasonable expectation of privacy.[27] Although allowing the government access to historical cell site data to use as evidence in a criminal proceeding aids law enforcement, legislators must recognize the risks that flow from allowing the government to retrieve cell phone location information without probable cause. At least one study suggests that the public is losing confidence in their ability to control personal information, ultimately creating public discomfort with and suspicion of government surveillance.[28] If Congress declines to amend the statute, the idea of a "big brother" government watching its people may disturb the sensibilities of the public.[29] In 2012, cell phone providers responded to over 1.1 million federal, state, and local law enforcement requests for cell phone records,[30] with the public largely remaining unaware of the volume of these requests.

Part I presents the Supreme Court's Fourth Amendment jurisprudence regarding this issue, while Part II highlights the analytical problems the circuit courts have faced in attempting to reconcile Supreme Court decisions in order to decide historical cell site data cases. Finally, Part III presents potential resolutions of the proper standard for historical cell site data retrieval and urges Congress to reexamine the SCA's "specific and articulable facts" standard to better comport with society's privacy expectations.

I. The Supreme Court's Fourth Amendment Jurisprudence

A. Early Fourth Amendment Jurisprudence

The Supreme Court's original Fourth Amendment jurisprudence was heavily tied to common-law trespass. In *Olmstead v. United States*,[31] the Court held that attaching wiretaps to telephone wires on public streets was not a Fourth Amendment search because "[t]here was no entry of the houses or

this Note, the actual precision of historical cell site data is debated, as it depends on the number of towers in a given area.

27 For a discussion on the historical record regarding the framing of the Fourth Amendment, see generally Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979 (2011).

28 *See infra* note 137 and accompanying text.

29 Justice Sotomayor noted the potential problems arising from the government watching the public in her concurrence in *United States v. Jones*: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *cf.* Smith v. Maryland, 442 U.S. 735, 751 (1979) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide.") (Marshall, J., dissenting).

30 Joe Palazzolo, *Appeals Court Will Reconsider Ruling on Cellphone Tracking*, Wall St. J. L. Blog (Sept. 4, 2014, 1:46 PM), http://blogs.wsj.com/law/2014/09/04/appeals-court-will-reconsider-ruling-on-cellphone-tracking/.

31 277 U.S. 438 (1928).

offices of the defendants."[32] The Supreme Court moved away from this exclusively property-based approach in *Katz v. United States*[33] when it held that "the Fourth Amendment protects people, not places."[34] In *Katz*, the attachment of an eavesdropping device to a public telephone booth in order to listen to and record the defendant's words was found to be a search and seizure within the Fourth Amendment.[35]

Justice Harlan's *Katz* concurrence developed an influential two-pronged test to determine the scope of the Fourth Amendment's protection. First, a person must have "exhibited an actual (subjective) expectation of privacy," and second, society must consider the expectation to be "reasonable."[36] However, courts have since largely ignored, or at least deemphasized, the first prong and instead have given more weight to the second prong.[37]

Even though *Katz* held that a telephone *conversation* from a public telephone is entitled to a reasonable expectation of privacy, the Court has not extended that Fourth Amendment protection to telephone *numbers*, even when dialed from an individual's private phone.[38] In 1979, the Court held in *Smith v. Maryland*[39] that a person has no reasonable expectation of privacy in information voluntarily turned over to a third party. There, police installed a pen register without a warrant in order to determine the identity of a person who had made threatening phone calls to a robbery victim, claiming that he was the one who robbed her.[40] The Court found no legitimate expectation of privacy regarding numbers dialed on a phone, as the numbers were turned over to a third party, the telephone company.[41] The Court further found that even if the defendant harbored a subjective expectation that the

32 *Id.* at 464.

33 389 U.S. 347 (1967), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

34 *Id.* at 351.

35 *Id.* at 347.

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

37 *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(c) (5th ed. 2014) (noting that "little attention has been given to the independent significance of the first factor or to precisely how it is to be interpreted"); *see also* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis . . . which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'" (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring))).

38 Jacob T. Whitt, Note, *Cell Phones as an Eye of the Government:* In re Application of the United States for Historical Cell Site Data, 88 TUL. L. REV. 831, 832 (2014).

39 442 U.S. 735 (1979).

40 *Id.* at 737. A pen register is an apparatus a telephone company can use to automatically record outgoing numbers dialed from a particular phone line, as well as the numbers of incoming calls. John Applegate & Amy Grossman, *Pen Registers After* Smith v. Maryland, 15 HARV. C.R.-C.L. L. REV. 753, 753 (1980).

41 *See Smith*, 442 U.S. at 743–44 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." (citing United States v. Miller, 425 U.S. 435, 443 (1976))).

numbers would remain private, society was not prepared to recognize that expectation as "reasonable," because when the defendant conveyed the numerical information to the telephone company in the normal course of business, he assumed the risk that the information may be turned over to law enforcement.[42] Therefore, the Court held that installing the pen register without a warrant did not violate the Fourth Amendment.[43]

B. Jones*: A Return to Common-Law Trespass*

In *United States v. Jones*, the Court returned to the common-law trespassory analysis of the Fourth Amendment and noted that Justice Harlan's reasonable-expectation-of-privacy test in *Katz*, which protects persons and their private conversations, was not "intended to withdraw any of the protection which the Amendment extends to the home."[44] *Jones* involved a defendant who the government suspected was involved in drug trafficking; the government obtained a search warrant to install a GPS tracking device on the bottom of the defendant's wife's car.[45] Government agents installed the device while the car was parked in a public parking lot eleven days after the warrant issued, even though the warrant authorized installation within ten days.[46] The government tracked the movement of the car for twenty-eight days following installation. The district court only excluded data obtained while the car was parked at the Joneses' home, while admitting the remainder of the evidence under *United States v. Knotts*.[47] That case[48] held that a "person trav-

42 *Id.* at 745–46.

43 *Id.*

44 United States v. Jones, 132 S. Ct. 945, 951 (2012) (quoting Alderman v. United States, 394 U.S. 165, 180 (1969)).

45 *Id.* at 948. Although the vehicle was registered to the wife, the defendant was the "exclusive driver" of the vehicle; the Court declined to consider the significance of the vehicle's registration status. *Id.* at 949 n.2.

46 *Id.* at 948.

47 *Id.*

48 United States v. Knotts, 460 U.S. 276 (1983). *Knotts* involved a challenge to the use of an electronic tracking device or "beeper" that was concealed in a container of chloroform. ROLANDO V. DEL CARMEN, CRIMINAL PROCEDURE: LAW AND PRACTICE 249 (9th ed. 2014). The beeper was already inside the container when the man suspected of manufacturing controlled substances purchased the chloroform from the chemical manufacturer. *Id.* Law enforcement tracked the movements of the container to a location in or near Knotts's secluded cabin, and with that information the state narcotics agents were able to secure a search warrant to search the suspect's drug laboratory. *Id.* In that case, the Court found that no Fourth Amendment concern was implicated because the drug manufacturers had no reasonable expectation of privacy while the vehicles were in plain view on the public highway. *Id.* According to the Court, the location of the container had been voluntarily conveyed to the public, but the court left open the question of monitoring vehicles in private places. *Id.*

In a subsequent "beeper" case decided one year later, United States v. Karo, 468 U.S. 705 (1984), the Court held that the installation of a beeper in a container, when consent of the original owner of the container was obtained and the container was then sold to a buyer who was unaware of the beeper's presence, was not a search or seizure protected by

eling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[49]

However, because the Supreme Court found that a vehicle is an "effect" under the Fourth Amendment, it held that the government's installation of the device on the vehicle and its subsequent use of the device to monitor the vehicle's movements was a "search" in violation of the Fourth Amendment.[50] Writing for the majority, Justice Scalia focused on the physical occupation of private property for obtaining information to explain the Court's decision, but noted that trespass is not the exclusive test for Fourth Amendment searches; rather, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[51] As the Court has not departed from its precedent establishing that visual observation is constitutionally permissible,[52] Justice Scalia left open the question of whether electronic surveillance without a trespass could be an unconstitutional invasion of privacy.[53]

Justices Sotomayor and Alito, however, recognized in their respective concurrences in *Jones* the broader issue that physical intrusions are not necessary for most forms of surveillance, and therefore, that the Fourth Amendment is concerned with more than trespassory intrusions on property.[54] Justice Sotomayor suggested that the idea that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties may need reconsideration because it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties."[55] The better question, she wrote, would be "whether people reasonably

---

the Fourth Amendment. *Id.* In that case, the beeper was used to track the container to several places, including private residences. *See* DEL CARMEN, *supra*, at 249. Because the government's contact with the container occurred prior to transfer to the defendant, the majority concluded that the installation of the beeper did not amount to a search or seizure; rather, the defendant "accepted the container as it came to him, beeper and all" and could not therefore object to its presence. *See Jones*, 132 S. Ct. at 952 (discussing *Karo*). However, the *Karo* Court did find that the government's use of a beeper to track constituted a search to the extent that that it revealed information about the interior of a *private* residence. *See* Chamberlain, *supra* note 8, at 1763 n.115.

49 *Knotts*, 460 U.S. at 281.

50 *Jones*, 132 S. Ct. at 949.

51 *Id.* at 953.

52 *See* Kyllo v. United States, 533 U.S. 27, 31–32 (2001).

53 *Jones*, 132 S. Ct. at 953–54. However, Justice Scalia remarked in a footnote that the majority's theory of the Fourth Amendment is not that a technical trespass is required. *Id.* at 953 n.8.

54 *Id.* at 954–57 (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring in the judgment).

55 *Id.* at 957 (Sotomayor, J., concurring). Instead, Justice Sotomayor indicated that it should not be assumed that information voluntarily disclosed to any member of the public automatically forfeits Fourth Amendment protection. *Id.* Justice Sotomayor cited Justice Marshall's dissent in *Smith v. Maryland*, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting), in which he wrote that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." *Id.*

expect that their movements will be recorded and aggregated in a manner that enables the [g]overnment to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[56]

Justice Alito also argued for an analysis that would better keep pace with present-day Fourth Amendment concerns regarding uses of new technologies. In his view, *Jones* should have been analyzed by asking "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring" of the vehicle's movements.[57] Of course, this framework would leave some uncertainty as to whether a certain period of time for surveillance constitutes a Fourth Amendment search—as "long-term monitoring" has never been defined. However, as Justice Alito argued, in the case of uncertainty, authorities may always seek a warrant by showing probable cause.[58] He specifically alluded to the issue of privacy in the cell phone context, where smart phones equipped with GPS technologies permit carriers to track and record users' locations; he suggested that the best solution to privacy in this context may come from Congress, which is better suited to create bright line rules.[59]

C. Riley*: Protecting Cell Phone Contents from Warrantless Searches*

In the recent decision of *Riley v. California*,[60] the Supreme Court addressed privacy in the cell phone context, but with respect to content rather than transmission. In *Riley*, a police officer seized Riley's cell phone upon discovering it in Riley's pants pocket during a search incident to arrest.[61] The officer then proceeded to access the information contained on

56 *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

57 *Id.* at 958 (Alito, J., concurring in the judgment). Under this framework, while a short-term monitoring of movements may accord with societal expectations of what is reasonable, long-term monitoring would be more likely to impinge on society's expectations of privacy. *Id.* at 964; *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness." (internal quotation marks omitted)). It may be the case that at least five Justices (Alito, Breyer, Ginsburg, Kagan, and Sotomayor) are ready to find that prolonged tracking is a search by endorsing some version of the D.C. Circuit's "mosaic theory" of Fourth Amendment protection. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320–21 (2012); *see* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945. From *Maynard*, the D.C. Circuit's mosaic theory can be used to analyze searches "as a collective sequence of steps rather than as individual steps" to find a Fourth Amendment violation. Kerr, *supra*, at 313.

58 *Jones*, 132 S. Ct. at 964.

59 *Id.* at 963–64 ("To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.").

60 134 S. Ct. 2473 (2014). The Supreme Court considered a companion case, *United States v. Wurie*, together with *Riley v. California*, but as they both raise the same legal question, they will collectively be referred to in this Note as "*Riley*."

61 *Id.* at 2480.

the phone and recognized repeated appearances of the letters "CK"—either in text messages or a contacts list—that the officer believed was short for "Crip Killers," a slang term for members of the Bloods gang.[62] At the police station, investigators found photo and video evidence on the phone that linked Riley to a shooting from a few weeks earlier.[63] The prosecutors sought to enhance Riley's sentence based on the information obtained from the cell phone.[64]

Citing *Kentucky v. King*,[65] the *Riley* Court explained that "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[66] The exception relevant in *Riley* was a warrantless search conducted incident to a lawful arrest, which allows a search of the area under the arrestee's "immediate control" to protect officer safety or to prevent destruction of evidence.[67] However, the Court recognized that cell phones do not further the same governmental interests—such as officer safety and evidence destruction—and that cell phones implicate greater individual privacy interests than physical searches.[68] The Court disagreed with the government's assertion that cell phone data is "materially indistinguishable" from the information discoverable about a person from certain physical items, such as purses, wallets, and address books.[69] *Riley* does not preclude officers from examining the physical aspects of the phone to ensure nothing on it can be used as a weapon.[70] But because the *contents* within the phone pose no risk of bodily harm to the officer, inspection of the contents cannot be justified without a warrant.[71] The Court was concerned with protecting individuals from the inherent qualities of cell phones that could allow private information to be conveyed "far more than previously possible."[72]

The Court also addressed the government's concern about evidence destruction. The government argued that a defendant may be able to use encryption or have the information within a cell phone wiped remotely, but

62 *Id.*

63 *Id.* at 2480–81.

64 *Id.* at 2481.

65 Kentucky v. King, 131 S. Ct. 1849 (2011).

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

67 *Id.* at 2482–83.

68 *Id.* at 2488.

69 Andrew Serwin et al., *Courts Defer to Individual Privacy Interests by Requiring Warrant to Obtain Cell Phone Data and Cell Site Records in* Riley *and* Davis, BLOOMBERG BNA 2 (July 30, 2014), *available at* http://www.mofo.com/~/media/Files/Articles/140730CourtsDefertoIndividualPrivacy.pdf.

70 *Riley*, 134 S. Ct. at 2478.

71 *Id.* Cases where law enforcement is at risk of physical harm are to be left to case-specific exceptions to the warrant requirement, such as the exception for exigent circumstances. *Id.* at 2486; *see, e.g.*, Warden v. Hayden, 387 U.S. 294, 298–99 (1967) ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.").

72 *Riley*, 134 S. Ct. at 2479.

the Court found that both of these methods of information protection were beyond what an arrestee would be able to achieve upon arrest.[73] The Court further explained that "wiping" can be prevented simply by disconnecting the phone from the network, either by removing the battery or by placing the phone in a place that isolates the phone from radio waves.[74] Furthermore, even if law enforcement officers are in a "now or never" situation, they may still be able to rely on another recognized exception—the exigent circumstances exception—in order to search the phone immediately in cases where remote wiping is imminent.[75] The exigent circumstances exception requires courts to determine whether an emergency situation can justify a warrantless search in certain cases.[76]

The Court very briefly mentioned the historic location information that cell phones also reveal to allow "reconstruct[ion] [of] someone's specific movements down to the minute,"[77] but it did not address the constitutionality of using 18 U.S.C. § 2703(d) to obtain historical cell site location data from third-party cellphone providers.[78] The Court also mentioned in a footnote that since the two cases in *Riley* involved searches incident to arrest, the Court did not have to reach the question of "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[79] The Court's footnote alludes to what Professor Orin Kerr calls the "mosaic theory" of the Fourth Amendment, which asks whether a collection of acts together amounts to a Fourth Amendment violation as opposed to an assessment of each step independently.[80] Although the Supreme Court has not yet adopted this approach, if the Court takes up the issue before Congress defines the boundaries of cell phone privacy with respect to historical cell site data, the "mosaic theory" may be a way to reach a just result in a difficult case.[81]

Finally, the Court acknowledged that although *Riley* would arguably have some impact on the law enforcement's ability to combat crime, the holding "is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search."[82] Like in *Jones*, Justice Alito once again pointed out in his concurrence that it may be

73 Serwin et al., *supra* note 69, at 2.

74 *Riley*, 134 S. Ct. at 2487.

75 *Id.*

76 *Id.* at 2494.

77 *Id.* at 2490.

78 *See supra* note 13 and accompanying text.

79 *Riley*, 134 S. Ct. at 2489 n.1.

80 *See* Kerr, *supra* note 57.

81 However, Kerr notes that the "mosaic theory" may have implementation problems in practice. *Id.* at 346 ("[T]he theory raises so many novel and puzzling new questions that it would be difficult, if not impossible, to administer effectively as technology changes.").

82 *Riley*, 134 S. Ct. at 2493.

time for the legislature to step in in order to balance the privacy interests of individuals against the needs of law enforcement.[83]

II. CURRENT TREATMENT OF HISTORICAL CELL SITE DATA

A. Third and Fifth Circuit Precedent

For the most part, the caselaw related to historical cell site data has occurred largely at the district court level,[84] but both the Fifth and Third Circuits have settled the issue within their jurisdictions.[85] The Fifth Circuit has declined to extend *Riley*'s holding regarding the *contents* within cell phones to historical cell site information.[86] The Fifth Circuit's leading precedent is still *In re Application of the United States for Historical Cell Site Data* (*In re Historical Cell Site Data*), which held that cell phone holders do not have a constitutionally protected interest in the location records providers keep.[87] Therefore, the *In re Historical Cell Site Data* court reversed the district court's adoption of a magistrate judge's ruling denying governmental access to historical cell site information.[88] In the Fifth Circuit's view, because cell phone users know that providers retain historical cell site information and "will turn it over to the police if they have a court order," cell phone users have "voluntarily" conveyed the cell site data whenever calls are made from their phones.[89] The court assumed that cell phone holders are sophisticated enough to understand that cell phone providers retain historical cell site data and will turn it over to law enforcement. However, it is debatable whether

83 *Id.* at 2497 (Alito, J., concurring) ("In light of these [modern cell phone] developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment.").

84 *See* Anderson, *supra* note 5.

85 *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010). The Second Circuit held in 2013 that § 2703(d) was not "clearly unconstitutional" and therefore allowed evidence obtained by an officer acting in reliance on the statute to be admitted under the good faith exception to the exclusionary rule. United States v. McCullough, 523 Fed. App'x 82, 83 (2d Cir. 2013). Some district courts in the Second Circuit treat the law in that circuit as supporting the conclusion that orders issued under § 2703(d) are covered by the good faith exception. *See, e.g.*, United States v. Mack, No. 3:13-cr-00054, 2014 U.S. Dist. LEXIS 159686, at *4 (D. Conn. Nov. 13, 2014); United States v. Serrano, No. 13 Cr. 58, 2014 U.S. Dist. LEXIS 81478 (S.D.N.Y. June 10, 2014).

86 *See, e.g.*, United States v. Guerrero, No. 13-50376, 2014 U.S. App. LEXIS 17584, at *13 (5th Cir. Sept. 11, 2014) ("[F]or a Supreme Court decision to change our Circuit's law, it must be more than merely illuminating with respect to the case before [the court] and must unequivocally overrule prior precedent." (second alteration in original) (quoting Tech. Automation Servs. Corp. v. Liberty Surplus Ins. Corp., 673 F.3d 399, 405 (5th Cir. 2012)) (internal quotation marks omitted)).

87 724 F.3d 600 (5th Cir. 2013).

88 *Id.* at 615.

89 *Id.* at 614.

the public is actually aware of or has even thought about their cell phone providers' practices.[90]

In re Historical Cell Site Data echoed the Third Circuit's 2010 decision in *In re United States for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government*,[91] which also reversed an order declining to provide historical cell site data.[92] Although the Third Circuit has treated historical cell site data similarly to how the Fifth Circuit has in allowing the "specific and articulable facts" standard to govern the disclosure of the information, because the magistrate judge asserted that a cell phone can act like a tracking device to disclose movement and location information, the court devoted substantial analysis to doubting this assertion.[93]

There is a general disagreement as to how accurately historical cell site data can reveal the location of a person carrying a cell phone. Given the various applications on smartphones that pull location data, it is plausible that in conjunction with the regular cell phone tower information, the cell phone provider could pinpoint the location of a person within several feet if it wanted to. But it is not clear that the government has ever actually received the more precise location information from applications on the phone through a § 2703 order under the Stored Communications Act.[94] Professor Kerr's sense is that cell providers do not "track every location a person goes; they only track where the phone was when a communication

90 The public may be more suspicious of cell phone providers in the wake of Edward Snowden's 2013 leak of documents regarding top-secret government surveillance programs. If the public was not on notice before, it should be now, given the media's attention to the leak. *See, e.g.*, Anthea Mitchell, *3 Reasons Americans Fear Government*, WALL ST. CHEAT SHEET (Nov. 15, 2014), http://wallstcheatsheet.com/politics/3-reasons-americans-are-so-suspicious-of-government-monitoring.html/?a=viewall ("To have true privacy, most Americans seem to believe they'd need to step back into the dark ages, taking a sword . . . to their . . . cell phone . . . . That is how the world changed, or at least how perceptions began to change more rapidly, after former NSA contractor Edward Snowden released his documents on government surveillance."); *cf.* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/#.

91 620 F.3d 304 (3d Cir. 2010).

92 Serwin et al., *supra* note 69, at 4 (noting that "[t]he Fifth Circuit's opinion echoes" *In re U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*).

93 *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010) ("There is no evidence . . . that historical [cell site data], even when focused on cell phones that are equipped with GPS, extends to that realm."). Cell site information was believed to only provide a "rough indication" of a user's location at the time a call was placed or received, although testimony of an FBI agent revealed that the records could be used to show the times that a person is generally in their home based on the lack of switching from one tower to another. *Id.* at 311–12.

94 Some commentators assert that the state of technology is such that the records disclosed may be quite precise. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."); *supra* note 26 and accompanying text.

was made."[95] Whether or not the historical cell site information can be characterized as a "tracking device" is important with respect to application of the SCA, which authorizes disclosure of "wire or electronic communication."[96] Since historical cell site data is not a form of wire communication, the data must fall within the "electronic communication" part of the statute.[97] However, because the definition of "electronic communication" excludes from its reach "any communication from a tracking device," the government may not compel disclosure under the SCA if the information conveyed from the device could be used to determine the movements of cell phone users.[98]

Although opponents of application of § 2703(d) to historical cell site data argue that the data can be likened to tracking information[99]—similar to the information collected from the GPS that was used to track the defendant in *Jones*[100]—the Fifth and Third Circuits have instead asserted that historical cell site data is considered a "business record" and therefore must be analyzed under that line of Supreme Court precedent.[101] The court in *In re Historical Cell Site Data* reasoned that the location data is a "business record" because the service provider "collects and stores historical cell site data for its own business purposes . . . on its network" and the government has never required that such records be kept.[102] Historical cell site data, unlike the GPS in *Jones*, does not involve a physical trespass because the information can be accessed remotely; although like a GPS, it may be able to provide information regarding individuals' locations in private spaces.[103]

---

95 Kerr, *supra* note 7. The accuracy of cell site data depends partly on the range of the coverage area of each cell tower, which means that a higher number of towers in an area will increase precision. *See The Electronic Communications Privacy Act (ECPA) Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 33 (2013) (statement of Catherine Crump, Staff Attorney, ACLU) [hereinafter *Electronic Communications Privacy Act Hearing*] ("[T]he latest generation of cellular towers now may cover an area as small as a tunnel, a subway, a specific roadway, a particular floor of a building, or even an individual home or office.").

96 Stored Communications Act, 18 U.S.C. § 2703(d) (2012).

97 *See* Chamberlain, *supra* note 8, at 1758.

98 *See id.*

99 *See, e.g.*, Anderson, *supra* note 5.

100 *See generally* United States v. Jones, 132 S. Ct. 945 (2012) (holding that installing a GPS tracking device on an individual's vehicle to monitor the car's movements constituted a search under the Fourth Amendment).

101 *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (vacating the district court's order for treating historical cell site information as tracking information rather than as a "business record"); *see also In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 309–10 (3d Cir. 2010) (rejecting the magistrate judge's characterization of historical cell site data as a "tracking device").

102 *In re U.S. for Historical Cell Site Data*, 724 F.3d at 611–12.

103 *But see* Kerr, *supra* note 7 (arguing that cell-site records are not "sufficiently precise" to detail whether an individual is within a particular space).

B. Eleventh Circuit Finds Reasonable Expectation of Privacy in Cell Site Data

The Eleventh Circuit's decision in *United States v. Davis*,[104] decided less than one month before *Riley*, has been vacated and will be reheard en banc. Its outcome on rehearing will be important because it might eliminate the circuit split. In *Davis*, the district court admitted historical cell site data that was obtained without a warrant, but on appeal the Eleventh Circuit panel questioned prior understandings of Fourth Amendment protection limitations and found that the government's warrantless gathering violated Davis's reasonable expectation of privacy.[105] In the panel opinion, Judge David B. Sentelle[106] reasoned that under the "privacy theory" of the Fourth Amendment, an invasion of privacy occurs when the government comes to know something "private in nature."[107] Such an invasion can occur when the government aggregates and analyzes so much public information that it learns something that would otherwise be private (i.e., the mosaic theory adopted in *Maynard* and alluded to in the *Jones* concurrence).[108] If no aggregation has occurred, the government can still violate the Fourth Amendment by learning something specific and private about a person.[109] Aggregation aside, *Davis* extended *Jones* because it concluded that "even a single point of cell site location data is presumptively private."[110] Further, even if the government obtains a type of record that only *might* reveal something private, aggregating any amount of information of that type of record is a search that requires a warrant.[111] Even though a physical trespass had not occurred in *Davis*, the Eleventh Circuit treated as instructive the *Jones* "mosaic theory" analysis from Justice Alito's concurrence.[112] Although a car's movements may be publicly observed, information obtained through the long-term monitoring of the vehicle over several weeks can be aggregated, violating an individual's reasonable expectation of privacy.[113]

The government's retrieval of Davis's historical cell site data was a search because it could be used to find out facts that were "private in nature," such as when he was "near the home of a lover" or other places deemed private in

104 754 F.3d 1205 (11th Cir. 2014), *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014).

105 *See* Serwin et al., *supra* note 69, at 3.

106 Judge Sentelle is a United States Circuit Judge for the District of Columbia who was sitting by designation.

107 Kerr, *supra* note 7 (quoting *Davis*, 754 F.3d at 1216).

108 *Id.*

109 *Id.* Even though the majority in *Jones* used the trespass theory to decide the case, four Justices concurred that the same result could have been reached under the privacy theory. *See* Serwin et al., *supra* note 69, at 3 (citing United States v. Jones, 132 S. Ct. 945, 958 (2012)).

110 Serwin et al., *supra* note 69, at 4.

111 *See* Kerr, *supra* note 7.

112 *See* Serwin et al., *supra* note 69, at 3.

113 *Id.*

nature.[114] Under this view, aggregation of historical cell site data has the potential to reveal more private information than could otherwise be obtained from retrieving only "pieces of information" about a person's location.[115] According to Kerr, Judge Sentelle's view that aggregating cell cite records may *potentially* disclose private facts to find a search is contrary to the Supreme Court's decision in *United States v. Karo*, which stated: "[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment . . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."[116]

Interestingly, while the government argued that *Jones* was distinguishable and that the Fourth Amendment was not violated because GPS is *more* precise than historical cell site data, the argument backfired; the court found this contrary to the purposes for seeking location evidence at all.[117] If historical cell data could be used to bolster a criminal conviction, then it was not too imprecise to violate an individual's reasonable expectation of privacy.[118]

Where does *Davis* leave courts? Because it does not require courts to engage in factual inquiries as to whether a "specific context of where the phone user was—such as whether on public or private property" will matter in a given case, the implication of *Davis* is that a warrant would be necessary to obtain cell site location data, but not surveillance camera footage—even where both similarly placed a defendant at the scene of a crime.[119] If the Eleventh Circuit's en banc opinion upholds the panel decision, then certain information about a person's location will be considered inherently private and therefore not discoverable absent a warrant, even though similar information about the person may already be in the public domain.[120]

The Eleventh Circuit panel is not alone in the battle to find a protectable privacy interest in historical cell site data. A federal magistrate judge in the Northern District of California struggled with the issue, given a lack of guidance from the Ninth Circuit and the conflict between the Fifth and Eleventh Circuits.[121] The judge requested explanation from the U.S. Attorney's Office and the San Francisco federal defender regarding why the government believed it did not have to obtain a search warrant to retrieve cell site records.[122] Some states have reacted to the issue since *Jones*. Colorado,

114 Kerr, *supra* note 7 (quoting United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014), *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014)).

115 *See* Serwin et al., *supra* note 69, at 3.

116 United States v. Karo, 468 U.S. 705, 712 (1984).

117 *See* Serwin et al., *supra* note 69, at 3.

118 *Id.*

119 *Id.* at 4.

120 *See id.*

121 *See* Hanni Fakhoury, *A National Consensus: Cell Phone Location Records Are Private*, EFF (July 29, 2014), https://www.eff.org/deeplinks/2014/07/constitutionally-important-consensus-location-privacy.

122 *Id.*

Maine, Minnesota, Montana, and Utah have all passed statutes that require law enforcement to obtain a search warrant before obtaining historical cell site data information from cell providers.[123] In Massachusetts and New Jersey, the highest state courts have held that their state constitutions require a warrant for the information.[124]

However, some federal district courts have expressly denied the persuasive authority of the Eleventh Circuit's *Davis* decision since it was vacated. The Northern District of Illinois denied the defendants' motion to suppress historical cell site data information that was collected by the government pursuant to three § 2703(d) requests.[125] In rejecting *Davis*, the court instead chose to lean on the Fifth Circuit's *In re Historical Cell Site Data* decision to find that court-ordered cell location data orders fit squarely within the SCA.[126] However, application of the mosaic theory from Justice Alito's *Jones* concurrence may have been appropriate in this case, as the government in the case received data for a ten-month period. Ten months of monitored location data would arguably be considered "long-term" and sufficient to violate a person's reasonable expectation of privacy.[127]

Meanwhile, the Fourth Circuit is considering *United States v. Graham*, which was decided in the District of Maryland in 2012 after the *Jones* decision.[128] Pointing to *Jones* and other established precedent,[129] the district court relied on the third-party doctrine—much like the Fifth Circuit—to find that there is no legitimate expectation of privacy in historical cell site location information, as that information is handed over "voluntarily" to the cell phone provider.[130] Since the information did not belong to the consumer

123 *Id.*

124 *Id.*; Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (finding an expectation of privacy in long term movements and holding that the expectation is not diminished merely because Sprint owned the records); State v. Earls, 70 A.3d 630 (N.J. 2013) (comparing the *Jones* concurrences to application of access to historical cell site information and acknowledging that since *Jones* was decided under a trespass theory, a warrant was not required).

125 United States v. Rogers, No. 13-CR-952, 2014 U.S. Dist. LEXIS 145980 (N.D. Ill. Oct. 9, 2014).

126 *Id.* at *10–11.

127 Judge Kocaras noted that the Seventh Circuit has not directly spoken on the cell site information question. *See* United States v. Thousand, 558 F. App'x 666, 670 (7th Cir. 2014) ("We have yet to address whether . . . cell-tower information that telecommunication carriers collect is protected by the Fourth Amendment.").

128 United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (denying defendant's motion to suppress historical cell site location data as evidence).

129 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *see also* United States v. Miller, 425 U.S. 435, 440–41 (1976) (holding that a bank's financial records for the defendant were not the defendant's "private papers" but instead were the "business records of the banks"; defendant could not assert ownership or possession of those records).

130 *Graham*, 846 F. Supp. 2d at 398 ("[H]istorical cell site location records . . . are not the 'private papers' of the [d]efendants—instead, they are the 'business records' of the

and instead belonged to the telecommunication company, the probable cause standard of the Fourth Amendment was deemed inappropriate. Therefore, the court reasoned that the "specific and articulable facts" standard of the Stored Communications Act governed, and ultimately denied the defendant's motion to suppress the information.[131] It will be interesting to see what the Fourth Circuit decides in light of *Riley*, especially since a district court case after *Riley* has also found that a defendant's Fourth Amendment rights were not violated when the government obtained cell location data pursuant to a § 2703(d) order.[132]

III. Problems Surrounding Privacy Protection of Historical Cell Site Data

A. Do Individuals "Voluntarily Disclose" Historical Cell Site Data?

Should the Eleventh Circuit come to the opposite conclusion in *Davis*, the Supreme Court would no longer have a circuit split ripe for resolution. However, even if the circuit split disappears, the tension behind the privacy issue surrounding historical cell site data will not. Although it may be difficult in practice to apply Justices Sotomayor and Alito's more flexible reasonable expectation analysis for aggregated information and long-term monitoring (i.e., the "mosaic theory" analysis), Justice Sotomayor's point that the categorical "voluntary" disclosure rule—or third party doctrine—may need revisiting should not fall on deaf ears. It does not follow from the simple choice to own a cell phone that the consumer has accepted that the information can be handed over to the government. As Justice Stewart recognized in dissent in *Smith v. Maryland*, "[a] telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service."[133] However, when a person purchases a cell phone, the purchaser is not given the option to tell the provider that it may not store location information, or even further that the provider may not release that information to others.[134] It would hardly seem just to say

cellular providers."). Furthermore, Judge Bennett rejected application of the "mosaic theory" as the majority in *Jones* did not endorse the theory, even though it was alluded to in Justice Alito's concurrence. *Id.* at 401.

131 *Id.* at 401 ("The fact of the matter is that in enacting the Stored Communications Act, Congress passed a law that rejects a warrant requirement for this type of information, but does require specific and articulable facts to be determined by a judicial officer.").

132 United States v. Giddins, No. WDQ-14-0116, 2014 U.S. Dist. LEXIS 140054 (D. Md. Sept. 30, 2014).

133 *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

134 As Justice Marshall noted in his dissent in *Smith v. Maryland*, even if it can be assumed that people "'typically know' that a phone company monitors calls for internal reasons . . . it does not follow that they expect this information to be made available to the public in general or the government in particular." *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (citation omitted). The same is true for cell site location data. *But see In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) ("Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call,

that Americans must forfeit privacy rights to take advantage of modern technology.[135] Justice Alito argued that individuals may find the "tradeoff" of privacy for new technology's convenience "worthwhile,"[136] but is it really safe to assume that society as a whole has come to accept this tradeoff?

Ninety-one percent of respondents to a Pew Research poll indicated that they believe "consumers have lost control over how personal information is collected and used by companies."[137] The survey also concluded that "context matters" when it comes to individuals deciding whether to disclose information or not.[138] But until it can be said with certainty that the public has "agreed" to lowered privacy expectations for the benefit of the use of better technology, an outright declaration that information has been "voluntarily" disclosed to a telecommunication company—and therefore has no reasonable expectation of privacy—should be avoided.

B. The "Specific and Articulable Facts" Standard Needs Reevaluation

Even if the Supreme Court never revisits the voluntary disclosure standard, as technology improves, court-ordered disclosures under § 2703(d) of the SCA may not be legal, as the associated cell phone records will essentially become the equivalent of tracking devices. Courts currently holding that probable cause is the appropriate mechanism for governing disclosure of historical cell site data—not the § 2703(d) "specific and articulable facts" standard of the SCA—concentrate on the breadth of the tracking device definition of the statute, and note that the device need only "permit tracking."[139] The demand by consumers for more data and improved service will

---

and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.").

135 Eric Samuel Heidel, *Warrantless GPS Tracking: Who Cares About Vehicle Transponders—What About Your Cell Phone?*, 8 J. INT'L COM. L. & TECH. 1, 2 (2013).

136 United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring). When considering the amount of information people post about themselves on the Internet for the public to see, it does seem to suggest that the way people value privacy has changed, or at least, that individuals' expectation of privacy has changed with respect to certain audiences and outlets. Take Facebook, for example. People post thousands of photos of their daily lives, but most people also have their privacy settings set to allow only their friends to view those pictures. Alyssa Newcomb, *Facebook Users Unwittingly Share More Personal Information, Study Finds*, ABC NEWS (Mar. 6, 2013), http://abcnews.go.com/Technology/facebook-lead-users-reveal-personal-information-study-finds/story?id=18667855. For analysis of the Fourth Amendment's application to the Internet, see Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010).

137 Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/#.

138 *Id.*

139 Chamberlain, *supra* note 8, at 1776 (citing *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info., 509 F. Supp. 2d 64, 74 (D. Mass.) (collecting cases), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007)).

only increase the number of towers in any given area, thereby increasing the precision with which the government can identify an individual's exact location through historical cell site data.[140] However, whether that information can be used to identify a person's location within several feet or several *hundred* feet, it would still arguably appear to fall within the definition of devices which "permit tracking" if it can give general geographic location specific enough to allow the evidence to be admissible in a criminal prosecution.[141]

If the gap between GPS and historical cell data records is truly closing,[142] Congress should not wait until the two are nearly indistinguishable to replace the "specific and articulable facts" standard with the Fourth Amendment's probable cause requirement. As the Court recognized in *Riley*, the warrant requirement is "an important working part of our machinery of government" and is not just "an inconvenience to be somehow 'weighed' against the claims of police efficiency."[143] The SCA's "specific and articulable facts" standard, which has been used to authorize retrieval of historical cell site data in court orders,[144] undermines the importance that has historically been placed on warrants in Fourth Amendment searches. Warrants are generally required to search homes and vehicles,[145] and it would not be an unreasonable burden in the historical cell site data context either, especially as warrants have become increasingly simple to retrieve through technological advances. For example, in *Riley*, the Supreme Court noted that there are jurisdictions "where 'police officers can e-mail warrant requests to judges' iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes.'"[146]

If additional circuits choose to follow the Fifth and Third Circuits, basic privacy expectations under the Fourth Amendment will be further eroded. A person's location truly is a "facet[ ] of American life that [has] been uniquely safeguarded from the intrusive interference and observation of government."[147] Judge Reinhardt of the Ninth Circuit wrote in his dissent in *United States v. Pineda-Moreno*[148] that in his thirty years on the bench, the courts have

140 *See Electronic Communications Privacy Act Hearing*, *supra* note 95, at 34.

141 Chamberlain, *supra* note 8, at 1776.

142 *See Electronic Communications Privacy Act Hearing*, *supra* note 95, at 33 (quoting statement of Professor Matt Blaze at the hearing on the ECPA).

143 Riley v. California, 134 S. Ct. 2473, 2493 (2014) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

144 *See* Anderson, *supra* note 5.

145 68 AM. JUR. 2D *Searches and Seizures* § 112 (2014) ("The Fourth Amendment demonstrates a strong preference for searches conducted pursuant to a warrant and generally prohibits warrantless searches." (footnote omitted)). In order to perform a search without a warrant, the search must fall within one of the "well-established exceptions" to the warrant requirement. *Id.*

146 *Riley*, 134 S. Ct. at 2493 (alteration in original) (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1573 (2013)).

147 *See Electronic Communications Privacy Act Hearing*, *supra* note 95, at 37.

148 United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Reinhardt, J., dissenting).

"gradually but deliberately reduced the protections of the Fourth Amendment."[149] As technology improves, the public ought to be disturbed by the idea that its privacy is left to judges relying on precedent involving old technology and existing laws, such as the SCA, which do not adequately consider the precision and accuracy that new technology can provide in disclosing a person's location. Furthermore, this issue will continue to be important, as the trend has been toward a significant increase in the number of court-ordered releases of cell phone records in recent years.[150]

The public would also benefit from having clear notice of the standards across different jurisdictions. In 2011, thirty-five ACLU affiliates that submitted public records requests with law enforcement groups around the nation found that standards varied widely for the showing law enforcement had to make for collecting different types of location information, not just historical cell phone data.[151] Individuals should not have to wonder whether they are in a jurisdiction that follows something less than a probable cause standard.

Congress should not leave it to courts to attempt to craft novel arguments as to why probable cause is the standard for historical cell site data. The courts are not fit to draw the boundaries necessary without completely overhauling Fourth Amendment jurisprudence, while legislatures are capable of drawing bright lines.[152] Though law enforcement would prefer the lower standard authorized by the SCA, Congress should expressly declare the historical preference for probable cause and the warrant requirement. A probable cause standard for compelling disclosure of historical cell site location information will still allow law enforcement to achieve its objectives while ensuring that Americans' privacy expectations are maintained in the cellular context. Since cell phone data can be used to discover information about a person that is "private in nature," such as whether a person is in an abortion clinic waiting room, attending an Alcoholics Anonymous meeting, or going to church, and the government cannot know ahead of time whether historical cell site data will convey this kind of information, requiring probable cause to obtain a warrant will better avoid that risk.[153]

149 *Id.*

150 Palazzolo, *supra* note 30. Verizon reported in a letter to Senator Ed Markey that cell phone record requests to the company have doubled in the past five years. *Id.*

151 *See Electronic Communications Privacy Act Hearing*, *supra* note 95, at 35–36. In an extreme example, the ACLU found that police in Lincoln, Nebraska are able to obtain even GPS data without a warrant based on probable cause. *Id.*

152 Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 37, 46 (Jeffrey Rosen & Benjamin Wittes eds., 2011) ("[L]egislatures . . . can promulgate bright-line rules concerning information collected under specific government powers, and they can explain the scope of the limitation and the contexts in which it is triggered.").

153 *See Electronic Communications Privacy Act Hearing*, *supra* note 95, at 39–40.

C. *The Geolocation Privacy and Surveillance Act*

Congress may be able to mitigate privacy concerns with respect to historical cell site data by passing the Geolocation Privacy and Surveillance (GPS) Act.[154] A bipartisan coalition led by Senator Ron Wyden, Representative Jason Chaffetz, and Senator Mark Kirk has reintroduced the bill to both houses of Congress after it was originally introduced in 2011.[155] The legislation would require law enforcement to obtain a warrant before being able to acquire "geolocation information" from a private company.[156] Its scope covers information created by electronic devices, such as cell phones, laptops, and GPS navigation systems, which can all be used to "infer information" regarding the location of an individual.[157] The GPS Act also creates criminal penalties for tracking the movements of an individual without a warrant, which are equivalent to current illegal wiretapping penalties.[158] The GPS Act would recognize certain exceptions to the warrant requirement, such as an emergency exception for when a person's life is in danger, an exception for parents to monitor their children, and an exception for lost or stolen electronic devices.[159]

The GPS Act has garnered support from the ACLU, the Electronic Frontier Foundation (EFF), the Digital Liberty Organization, and the Computer and Communications Industry Association (CCIA), among other groups.[160] The goal of the legislation is to give both private citizens and commercial entities, such as cell phone providers, "clear guidelines" regarding the circumstances in which geolocation information may be obtained and used.[161] After the GPS Act's reintroduction in January 2015 to the 114th Congress, it currently awaits consideration by the Senate and House Judiciary Committees and the House Intelligence Committee.[162]

---

154 *Geolocation Privacy and Surveillance ("GPS") Act*, RON WYDEN SENATOR FOR OR., http://www.wyden.senate.gov/priorities/gps-act (last visited Apr. 20, 2015) [hereinafter *GPS Act*].

155 *Id.*

156 *Id.* "Geolocation information" is defined as "information derived from a device that is not the content of a communication and 'could be used to determine or infer information regarding the location of the person.'" Privacy Tracker, *The Next Privacy Frontier: Geolocation*, IAPP (June 3, 2013), https://privacyassociation.org/news/a/the-next-privacy-frontier-geolocation/.

157 *See* Privacy Tracker, *supra* note 156.

158 *GPS Act*, *supra* note 154.

159 *Id.*

160 Press Release, Rep. Jason Chaffetz, Chaffetz Works to Protect Privacy with GPS Act (Mar. 21, 2013), http://chaffetz.house.gov/press-release/chaffetz-works-protect-privacy-gps-act.

161 *Id.*

162 *See* GPS Act, H.R. 491, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/491/text; *see also* GPS Act, S. 237, 114th Cong. (2015), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/237?q={%22search%22%3A%5B%22\%22GPS+Act\%22%22%5D}. The legislation was also reintroduced in the 113th Congress but ultimately never moved forward.

CONCLUSION

Although the concurrences in *Jones* suggest that the Supreme Court may be ready to find that aggregated historical cell site data over a long period constitutes a search in violation of the Fourth Amendment,[163] such a finding may have problematic implementation consequences in the long run.[164] The Supreme Court is not equipped to draw the bright lines needed to address the nuanced ways in which technology could violate an individual's reasonable expectation of privacy, even though some argue that *Riley* has provided the "catalyst" for the Supreme Court to decide other Fourth Amendment technology-related issues.[165]

Instead, Congress should pass the GPS Act because virtual searches are quickly replacing physical ones. Technological advances reveal that the current view of the Fourth Amendment is immaterial to most investigations.[166] A search involves looking for something; the form the search takes should be immaterial if it will reveal the same information as a physical search. The sooner this is recognized, the sooner we can return to the true privacy protections the drafters of the Fourth Amendment intended. Like the contents of a cell phone, if the government wants to learn the private whereabouts of an individual from historical cell site data, the answer should be simple: "get a warrant."[167]

* * *

POSTSCRIPT

As this Note went to press, the Eleventh Circuit in an en banc opinion vacated the prior decision in *United States v. Davis*, holding that probable cause is not required to retrieve cell phone location data.[168] Judge Frank Hull delivered the majority opinion writing that the stored telephone records serve compelling governmental interests and "are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses."[169] The court further noted that Davis had a diminished expectation of privacy in the phone records owned by MetroPCS and that, because the records were not his property, the production of those records did not entail a serious invasion of privacy.[170] The en banc court upheld Quartavius Davis's conviction under the good-faith exception, which pre-

163 *See supra* text accompanying notes 54–59.

164 *See* Kerr, *supra* note 57, at 346.

165 *See* Anderson, *supra* note 5.

166 Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE, *supra* note 152, at 11, 19.

167 Riley v. California, 134 S. Ct. 2473, 2495 (2014).

168 United States v. Davis, No. 12-12928, 2015 U.S. App. LEXIS 7385, at *32 (11th Cir. May 5, 2015).

169 *Id.* at *51.

170 *Id.* at *52–53.

cludes courts from suppressing evidence when law enforcement's conduct is based on a good-faith belief that the actions were legal under current law.[171]

Two judges dissented from the majority opinion on the Fourth Amendment question.[172] Judge Beverly B. Martin, writing for the dissent, wrote that the Fourth Amendment requires the government to get a warrant to retrieve historical cell site location information and that "[t]he judiciary must not allow the ubiquity of technology—which threatens to cause greater and greater intrusions into our private lives—to erode our constitutional protections."[173]

The opinion specifically noted that Davis was not tracked in real-time and that the records did not pinpoint Davis's precise location.[174] Thus, the court's ruling was carefully narrow. Some commentators suggest that although Davis was using old cell phone technology without GPS real-time tracking capability, lower courts may still read the opinion to leave smartphone users vulnerable to more precise tracking.[175] Although the decision eliminates the circuit split, it does not eliminate the public's interest in the issue and the need for a solution that takes account of the realities of modern technology.

171 *Id.* at *53.

172 *Id.* at *94.

173 *Id.* at *95.

174 *Id.* at *8–12.

175 Andy Greenberg, *Court's Reversal Leaves Phones Open to Warrantless Tracking*, WIRED (May 5, 2015, 5:37 PM), http://www.wired.com/2015/05/courts-reversal-leaves-phones-open-warrantless-tracking/ (citing Susan Freiwald, privacy law professor at San Francisco Law School).