# HISTORICAL CELLULAR LOCATION INFORMATION AND THE FOURTH AMENDMENT

NATHANIEL WACKMAN*

*Currently, there is a disagreement among courts as to whether section 2703(d) of the Stored Communications Act, which governs the disclosure and use of historical cellular location information, violates the Fourth Amendment. Increasingly, the federal government is using cellular phone companies' historical cellular location information—data communicated by a cellular phone to a cellular network, which identifies the location of a phone at a particular time—to investigate and prosecute crimes. This information can provide an accurate, historical record of a person's general whereabouts during the time period for which the data applies. Though the Fifth Circuit has held that section 2703(d) court orders are constitutional, several courts have found that the provision's "specific and articulable facts" requirement violates the Fourth Amendment. These courts prescribe that law enforcement secure a search warrant with the requisite showing of probable cause prior to obtaining the data.*

*This Note examines the controversy surrounding historical cellular location information and the Fourth Amendment. It begins by exploring the technology and law enforcement's interest in the information. This Note then surveys pertinent Supreme Court precedent and analyzes the major approaches taken by courts in addressing the use of this data. In particular, there are three approaches taken by courts: (1) use of the third-party doctrine, (2) treatment of the issue as a tracking case, and (3) use of the "mosaic theory" articulated in* United States v. Maynard.

*This Note contends that while the Fourth Amendment is likely not implicated by historical cellular location information, legislatures and law enforcement alike must take steps to strike the appropriate balance between privacy and security. It proposes that Congress amend the Stored Communications Act to include a statutory suppression remedy. This will provide a way to exclude evidence collected pursuant to faulty, conclusory, or false court orders. Additionally, this Note suggests that federal and state legislatures remedy excesses in the acquisition of historical cellular location information. Moreo-*

* J.D. Candidate, 2015, University of Illinois College of Law. A.B., 2006, University of Chicago. I would like to thank the editors and members of the *University of Illinois Law Review*, especially Marisa Young, Alex Garel-Franzen, and John Byers, for their invaluable contributions to this Note. Any and all errors that remain are mine alone. I dedicate this Note to my wife, Shewanna, for her endless patience, forgiveness, support, and love.

*ver, it recommends that law enforcement impose its own standards and require warrants prior to accessing the information sought. While a constitutional bar to this evidence may not exist, our rapidly changing notion of a "reasonable expectation of privacy" demands proactive and introspective action by legislatures and law enforcement.*

TABLE OF CONTENTS

## I. INTRODUCTION

On March 31, 2010, a man walking in the woods of rural Ashton, Maryland came upon the body of a man who had been brutally shot.[1] Ashton is in Montgomery County, a sprawling area which sits between Baltimore and Washington, D.C. Montgomery County is home to a number of members of *La Mara Salvatrucha*,[2] also known as MS-13,[3] an "extremely violent" criminal organization with an estimated 30,000 members worldwide.[4] The body was shortly thereafter identified as that of Felipe Leonardo Enriquez,[5] a twenty-five year-old purported MS-13 member known as "Zombie."[6] The federal government would later allege that Enriquez had possibly committed several violations of MS-13 rules—among them, covering up an MS-13 tattoo[7] and falsely claiming to have been an MS-13 member in Guatemala.[8] In response to these violations, Enriquez had been "green-lit," meaning that MS-13 leaders had ordered him killed.[9] This particular "green-light" had been issued from prison by an MS-13 leader incarcerated in El Salvador who had leadership responsibilities for certain Washington, D.C. based MS-13 cliques.[10] It was issued to Noe Machado-Erazo, an MS-13 member from

1. *Man's Body Found with Gunshot Wounds in Montgomery County*, WASH. POST, Apr. 1, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/31/AR2010033104363.html.

2. As the government explains, "[t]he name '*Mara Salvatrucha*' is a combination of several slang terms. The word '*Mara*' is the term used in El Salvador for 'gang.' [The gang has roots in El Salvador.] The phrase '*Salvatrucha*' is a combination of the words '*Salva*,' which is an abbreviation for 'Salvadoran,' and '*trucha*,' which is a slang term for the warning 'fear us,' 'look out,' or 'heads up.'" Indictment at 2, United States v. Aguilar, No. 10-256 (RMC) (D.D.C. Nov. 1, 2011).

3. MD. COORDINATION & ANALYSIS CTR., 2012 GANG THREAT ASSESSMENT 9 (2012), *available at* http://www.mcac.maryland.gov/resources/2012%20PUBLIC%20Gang%20Threat%20Assessment.pdf.

4. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Latin American Criminal Organization (Oct. 11, 2012) (internal quotation marks omitted), *available at* http://www.treasury.gov/press-center/press-releases/Pages/tg1733.aspx. In 2012, in recognition of their sophistication and "involvement in serious transnational criminal activities, including drug trafficking, kidnapping, human smuggling, sex trafficking, murder, assassinations, racketeering, blackmail, extortion, and immigration offenses," *id.*, MS-13 became the first "street gang" to be named a "transnational criminal organization" by the Treasury Department. Sam Quinones et al., *In a First, U.S. Labels MS-13 Street Gang 'Criminal Organization'*, L.A. TIMES L.A. NOW (Oct. 11, 2012, 1:52 PM), http://latimesblogs.latimes.com/lanow/2012/10/in-a-first-us-labels-ms-13-street-gang-criminal-organization.html.

5. Dan Morse, *Montgomery Police Tentatively ID Homicide Victim Found in Woods*, WASH. POST CRIME SCENE BLOG (Apr. 5, 2010, 5:01 PM), http://voices.washingtonpost.com/crime-scene/montgomery/moco-police-tentatively-id-vic.html.

6. United States v. Machado-Erazo, 986 F. Supp. 2d 39, 53 (D.D.C. 2013); Press Release, Office of Pub. Affairs, U.S. Dep't of Justice, Three MS-13 Leaders Found Guilty of Racketeering and Additional Charges for Multiple Murders and Attacks (Aug. 6, 2013), *available at* http://www.justice.gov/opa/pr/2013/August/13-crm-888.html.

7. Indictment, *supra* note 2, at 20.

8. *Machado-Erazo*, 986 F. Supp. 2d at 53.

9. *Id.* at 49 ("'MS-13 members are obligated, if they see a person that they know has a green light, to kill them,' and failure to do so could be grounds for punishment with a green light. Witnesses testified that the Normandie and Sailors cliques were aware of and bound by the green-light system.") (citation omitted). "Cliques" are smaller subsets of MS-13 "operating in a specific city or region," which function "under the umbrella rules of MS-13." Indictment, *supra* note 2, at 5. The "Normandy" and "Sailors" cliques were the two Washington, D.C.-based cliques at issue in this case. *Id.*

10. *Machado-Erazo*, 986 F. Supp. 2d at 47–48, 53.

Maryland.[11] On March 28, 2010, Machado-Erazo and Jose Martinez-Amaya, a fellow MS-13 member, drove Enriquez to remote Ashton, shot him multiple times, and left his body there.[12]

At Machado-Erazo and Martinez-Amaya's trial on federal racketeering charges, the government presented a variety of evidence to prove that Machado-Erazo and Martinez-Amaya were involved in an ongoing conspiracy, which included the murder of Enriquez. This evidence included the testimony of approximately fifty witnesses, including MS-13 members who cooperated as part of plea agreements,[13] as well as extensive wiretap and consensual recording evidence.[14] To buttress their case, however, the government introduced cellular phone records showing "that the cell phones used by defendants Machado Erazo, Jose Martinez Amaya, and a cooperating witness were in the remote area where the body of Felipe Enriquez was found on or about March 28, 2010."[15]

Several years prior, the government used similar technology in another case from the capital area. Antoine Jones openly owned a Washington, D.C. nightclub named "Levels," but the government suspected his main business interest was trafficking large amounts of cocaine from McAllen, Texas, into the Washington, D.C. area.[16] The Federal Bureau of Investigation-Metropolitan Police Department Safe Streets Task Force began an extensive investigation of Jones in 2004.[17] Over the course of 2004 and much of 2005, investigators used a host of techniques including: "surveillance, informants, installation of an electronic tracking device on Jones' vehicle, search warrants issued to electronic communication service providers for text messages to or from cellular telephones used by Jones and an alleged co-conspirator, and a Title III wire intercept,"[18] as well as a number of orders for cellular location information.[19] In October 2005, a raid at a Fort Washington, Maryland stash house, which investigators believed was tied to Jones, resulted in the seizure of 100 kilograms of cocaine.[20] Jones' first trial on federal drug charges ended in an acquittal.[21] His second trial resulted in a conviction

11. *Id.* at 46, 53; Press Release, U.S. Dep't of Justice, *supra* note 6.

12. *Machado-Erazo*, 986 F. Supp. 2d at 49 n.4, 53.

13. *Id.* at 43. Some to great personal danger. After one of the lead defendants in this case entered into a plea agreement, his sister was kidnapped in El Salvador as a warning to him to cease cooperating. *Id.* at 51.

14. *Id.* at 43.

15. United States v. Machado-Erazo, 950 F. Supp. 2d 49, 51 (D.D.C. 2013) (internal quotation marks omitted).

16. Henri E. Cauvin, *Cash and Cocaine, but No Conviction*, WASH. POST, Mar. 5, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/04/AR2007030401485.html; *see also* United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

17. *Maynard*, 615 F.3d at 549.

18. United States v. Jones, 451 F. Supp. 2d 71, 74 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

19. United States v. Jones, 908 F. Supp. 2d 203, 205 (D.D.C. 2012).

20. *Jones*, 451 F. Supp. 2d at 74.

21. *Jones*, 908 F. Supp. 2d at 205 n.1.

and a life sentence, but the use of evidence derived from a warrantless GPS tracking device on his car led the D.C. Circuit Court of Appeals to reverse his conviction,[22] which the Supreme Court later affirmed.[23] On the government's third trial of Jones, in addition to the other evidence they presented, prosecutors used cellular phone location data to tie Jones to the stash house where the cocaine had been found.[24]

These cases are two examples of how police and prosecutors are using historical location data from cellular telephone companies to investigate and prosecute crimes. This data, when interpreted properly, can provide a historical record of the location of a particular cellular telephone.[25] Since many people carry their cell phone on them at all times,[26] in effect, this data can provide a fairly accurate picture of a person's general whereabouts during the time period for which the data applies. The investigative and evidentiary possibilities of such information are innumerable. Records of a person's cell phone location can destroy alibis[27] and establish presence near a crime scene at the approximate time of the crime.[28]

Under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–12 (2012), law enforcement may seek a court order to compel disclosure of historical location data by a cellular phone company "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[29]

Criminal defendants, as well as some courts, have seized upon the "specific and articulable facts" requirement as violative of the Fourth Amendment.[30] In their view, getting this data should require law en-

22. *Id.*; *Maynard*, 615 F.3d at 567–68.

23. United States v. Jones, 132 S. Ct. 945, 948–49, 954 (2012).

24. Ann E. Marimow, *Judge Declares Mistrial in D.C. Area Drug Case*, WASH. POST, Mar. 4, 2013, http://articles.washingtonpost.com/2013-03-04/local/37433957_1_felony-drug-jurors-cocaine.

25. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATT'YS' BULL. 16, 16 (Nov. 2011). While writing this article, the author was an Assistant U.S. Attorney in the Western District of North Carolina.

26. "[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." Riley v. California, 134 S. Ct. 2473, 2484 (2014). *See also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

27. *See, e.g.*, State v. Patton, 419 S.W.3d 125, 129 (Mo. Ct. App. 2013) (describing the introduction of the "location of cell sites used by [the defendant's] cell phone in the time period surrounding the crime" in order "to establish that [he] was in the vicinity of the crime when it was committed, and not sleeping at his cousin's house as he claimed").

28. United States v. Machado-Erazo, 950 F. Supp. 2d 49, 51 (D.D.C. 2013) (describing the government's intention to use cell site location information in a murder trial to show "'that the cell phones used by defendants . . . were in the remote area where the body . . . was found'").

29. 18 U.S.C. § 2703(d) (2012).

30. *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) ("Compelled warrantless disclosure of cell site data violates the Fourth Amendment. . . . Accordingly, the Government's requests for that information under the SCA are denied.");

forcement to secure a warrant with the requisite showing of probable cause.[31] Prosecutors and other courts have defended the court order requirement. In their view, this information falls under either the third-party doctrine[32] or is simply not a search, since the phone merely conveys a person's public location—information which could be obtained by simply following a person around, an act which requires no legal process at all.[33]

Relatively few courts have decided this issue, though many will undoubtedly confront it in the coming years, as law enforcement use of cellular phone data has increased markedly.[34] Among courts who have decided it, the Fifth Circuit has found that the section 2703(d) court orders do not violate the Fourth Amendment.[35] The Eleventh Circuit briefly disagreed, creating a circuit split, though that decision has been vacated pending an en banc rehearing.[36] This reversed a lower court ruling, which found that the government must seek a warrant for this information.[37] The New Jersey Supreme Court[38] and the Massachusetts Supreme Judicial Court,[39] relying on their state constitutions, but using reasoning which may apply in a federal constitutional context, have found that law enforcement must seek a warrant in order to gain historical cellular location information.[40] Federal district and state courts of all levels have come down on both sides of the question.[41]

This Note examines the controversy over historical cellular location information. It will begin by discussing the technology and law enforcement's interest in it—what information can be obtained, how detailed and accurate it is, and how law enforcement uses it. The Note will then look at the relevant case law—both Supreme Court precedents, which may shed light on this question, as well as the holdings of courts which have examined it. This Note will then suggest that while the Fourth Amendment is likely not implicated by historical cellular location information, legislatures must be responsive and law enforcement must be introspective. With the "reasonable expectation of privacy" in data rapidly

Brief of the Appellant at 28, United States v. Davis, No. 12-12928 (11th Cir. June 24, 2013) (asking 11th Circuit for new trial on basis of admission and use of cellular location information obtained without a warrant).

31. *See infra* Part III.C.

32. *See infra* Part III.A.

33. *See infra* Part III.B.

34. *See* Jasmin Melvin, *Cell Phone Companies See Spike in Surveillance Requests*, REUTERS (July 9, 2012), http://www.reuters.com/article/2012/07/09/us-usa-wireless-surveillance-idUSBRE8680TW20120709.

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

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

37. *See In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010).

38. State v. Earls, 70 A.3d 630 (N.J. 2013).

39. Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014).

40. *See id.* at 850; *Earls*, 70 A.3d at 633.

41. *See infra* Parts III.A–C.

changing, legislatures and law enforcement must ask what they gain and what they lose by adhering to the "specific and articulable facts" standard. While a constitutional bar to this evidence may not exist, legislatures or law enforcement may want to impose a greater requirement on such information.

## II. BACKGROUND

### *A. What Is Historical Cellular Location Information?*

#### *1. What Is Historical Cellular Location Information and How Does it Work?*

Fourth Amendment cases and jurisprudence are very often fact- and context-specific.[42] In particular, precisely how the data is collected and what can be learned proves very important in assessing the Fourth Amendment implications of historical cellular location information. Therefore, exactly what can be obtained and used by law enforcement is an important threshold inquiry.

Historical cellular location information is, at its most basic, data communicated by a cellular phone to a cellular network, which identifies the location of that phone at a particular time.[43] Cellular phone networks allow for voice and data communication without a "wired" connection—in other words, cellular phones theoretically allow people to communicate using voice and data from anywhere in the world.[44] This is accomplished through the communication of a mobile station—typically a cellular phone—with a base station—this is the so-called "cell site"—through the use of electromagnetic waves.[45] The base station is in turn connected, via a base station controller, to the public switched telephone network, which allows for mobile phones to communicate with the telephone network (other cellular phones or landlines) at large.[46]

With this framework in mind, cellular phone location information generally comes in two types.[47] The first approach relies on the use of a global positioning system ("GPS") satellite receiver built into the phone.[48] This information can be extremely accurate, often able to locate

42. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442 (1976) ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents.").

43. *See* GOTTAPU SASIBHUSHANA RAO, MOBILE CELLULAR COMMUNICATION § 1.5 (2012).

44. *See id.*

45. *Id.*

46. *Id.*; *see also* O'Malley, *supra* note 25, at 20–21.

47. *See Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 50 (2013) [hereinafter *Blaze Testimony*] (statement of Matt Blaze, Associate Professor, University of Pennsylvania).

48. *Id.* at 51.

the receiver within a ten meter radius.[49] Its utility, however, is hampered by its unreliability when the receiver is located indoors and the GPS satellites are unable to "see" the receiver.[50] Furthermore, this GPS information is not always communicated to the wireless company on a regular basis—or at all[51]—nor do companies regularly collect and retain it.[52] In fact, a recent investigation by Senator Edward Markey of Massachusetts found that of the major wireless companies,[53] three companies did not retain this GPS data at all,[54] one retained it for two to three days,[55] and only one company stated that it retained the information for up to one year.[56]

The second approach is "network data." Network data is produced when a cellular phone communicates with a base station using electromagnetic waves.[57] Cellular phones do this in order to place and receive calls.[58] This is called "telephone" cellular location information and is collected only when a call is placed or received.[59] Cellular phones also need to communicate with the network, however, in order to judge signal

49. *Id.*

50. *Id.* at 52.

51. *Id.* ("Unfortunately, GPS, for all its promise, has a number of fundamental limitations. It relies on special hardware in the phone (particularly a GPS receiver chip) that is currently included *only* in the latest handset models and that generally is enabled for location tracking *only* when the phone user is explicitly using it to run a location-based application on the phone. Perhaps most importantly, GPS works reliably only outdoors, when the handset is in 'view' of several GPS satellites in the sky above.") (emphasis added).

52. *Id.* at 51.

53. The companies that responded to Senator Markey's request for information were U.S. Cellular, Sprint Nextel, T-Mobile, Lead Wireless/Cricket Communications, Verizon, AT&T, and C Spire Wireless. Press Release, Senator Edward Markey, For Second Year in a Row, Markey Investigation Reveals More than One Million Requests by Law Enforcement for Americans Mobile Phone Data (Dec. 9, 2013), *available at* http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data [hereinafter Markey Press Release].

54. The companies were U.S. Cellular, Letter from John C. Gockley, Vice President, Legal and Regulatory Affairs, U.S. Cellular, to Senator Edward Markey (Oct. 1, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_USCellular_CarrierResponse.pdf; AT&T, Letter from Timothy McKone, Exec. Vice President, Fed. Relations, AT&T, to Senator Edward Markey (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf (suggesting that the company, which has kept non individualized records in the past, no longer appears to retain this information); and T-Mobile and what was formerly Metro PCS, Letter from Tony Russo, Vice President, Fed. Legislative Affairs, T-Mobile, to Senator Edward Markey (Oct. 4, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_Tmobile_CarrierResponse.pdf. Additionally, Leap Wireless/Cricket Communications appears to not retain this information, though its response to Senator Edward Markey did not specifically address GPS information. *See* Letter from Robert J. Irving, Jr., Chief Legal & Admin. Officer, Cricket Commc'ns, Inc., to Representative Edward Markey (Oct. 7, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-07_Cricket.pdf.

55. This was C Spire Wireless. Letter from Benjamin M. Moncrief, Dir., Gov't Relations, C Spire Wireless, to Senator Edward Markey (Oct. 7, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_Cspire_CarrierResponse.pdf.

56. This was Verizon. Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Senator Edward Markey (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf.

57. *Blaze Testimony*, *supra* note 47, at 52–53.

58. RAO, *supra* note 43.

59. Commonwealth v. Augustine, 4 N.E.3d 846, 868 (Mass. 2014) (Gants, J., dissenting).

strength, network compatibility, user identification, and to "register [the] location" of the cell phone.[60] This process occurs periodically and automatically as long as the cellular phone is on.[61] This is known as "registration" cellular location information,[62] and, among other things, it will indicate the cell site with which a cellular phone is communicating.[63]

A cell tower sits in the middle of the area which it services, called a "cell."[64] This cell is typically hexagonal in shape.[65] Cell towers most commonly have three sets of antennae, with each set covering approximately 120 degrees of the cell.[66] This typical configuration can vary widely, however, with anywhere from one to six antennae providing service over an area of differing shapes and sizes.[67] Cellular phone location data can typically, at a minimum, provide information about what cell and cell sector antennae a cell phone was using when making or receiving a call.[68] Some years ago, this would have only given the loosest picture of where a person might be located. As cell sites have proliferated to handle increased traffic, especially in urban areas, their cell coverage area has shrunk.[69] As Professor Matt Blaze explained to a House subcommittee, a cell site

> can handle only a limited number of simultaneous call connections . . . . As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by their own [cell sites] and antennas.[70]

As the sectors shrink, the location and sector of the cell site in use becomes more valuable information. Additionally, wireless providers now have the capability, in some circumstances, to more accurately calculate location, even to within fifty meters, using the time and angle of arrival of the signal coming from the cellular phone.[71] It is unclear to what extent wireless providers actually practice this standard, or whether they retain information this precise.[72]

Cellular phones, however, do not always communicate with the *closest* tower, which complicates the picture provided by information

60. RAO, *supra* note 43, at § 1.6.3.

61. *Blaze Testimony*, *supra* note 47; RAO, *supra* note 43, at § 1.6.3 (describing how the procedure of a mobile phone "scan[ning] and select[ing] the strongest . . . signal sent by adjacent" cell sites, then "handshaking" with the strongest cell site "to identify the user and register its location . . . is repeated periodically as long as the mobile [phone] is on").

62. *Augustine*, 4 N.E.3d at 868 (Gants, J., dissenting).

63. *Blaze Testimony*, *supra* note 47, at 53.

64. RAO, *supra* note 43, at § 2.2.

65. *Id.*

66. *Id.* at § 1.5.

67. Matthew Tart et al., *Historical Cell Site Analysis—Overview of Principles and Survey Methodologies*, 8 DIGITAL INVESTIGATION 185, 186 (2012).

68. *Blaze Testimony*, *supra* note 47, at 53.

69. *Id.* at 54.

70. *Id.*

71. *Id.* at 56.

72. *Id.* at 57.

about the cell site with which a phone is communicating.[73] Typically, a particular cell site will have a "dominant" region and a "nondominant" region.[74] The dominant region will typically be a region with direct line of sight to the cell site and "no other cells of greater or equivalent power close by."[75] Within this region, the phone will "be unlikely to select any other cell."[76] The dominant region, however, will be a relatively small area of the total area that would potentially be served by the cell cite.[77] The nondominant region, meanwhile, will include the remainder of that potential area and will include regions where the cell site in question will not always communicate with the phone even if it is geographically the closest.[78] In areas that feature a large amount of cellular phone traffic and therefore contain a great number of cell sites, the effect of "clutter" in the form of line of sight or localized interference issues can cause phones to communicate with a site which is not the closest.[79] Furthermore, "[i]f there are other cells serving the area with similar signal strengths, the cell selected as serving by the [phone] may change frequently."[80] For the purpose of this Note, the bottom line of this technological analysis is that figuring out the cell site with which a phone is communicating is often only the beginning of the analysis involved in figuring out an approximate location.[81]

### *2. How Much and Why Is Historical Cellular Location Data Collected?*

Wireless providers are required by the Federal Communications Commission to locate cellular phones that call 911, but they are not required to keep historical records.[82] Companies do retain the historical data of the cell sites with which phones have communicated, however. For instance, AT&T retains this data for all its subscribers for five years.[83] In 2014, AT&T boasted of having 116.6 million wireless subscribers.[84] AT&T is hardly alone, as the other major wireless companies that re-

73. Tart et al., *supra* note 67, at 186.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. Various surveying techniques can give investigators tools to interpret the data more successfully and narrow the location within the area a cell site could potentially service. The accuracy of this information, however, can vary widely. Of course, cell site information can still be used almost definitively to exclude cell sites by showing that there is no geographic possibility that a phone could have been communicating with that site. *See generally id.* at 185–93.
82. *See* 47 C.F.R. § 20.18(e) (2012) (describing how mobile phone companies "must provide . . . the location of all 911 calls by longitude and latitude in conformance" with certain FCC-mandated "accuracy requirements").
83. Letter from Timothy McKone to Senator Edward Markey, *supra* note 54.
84. AT&T INC., 2Q 2014 AT&T BY THE NUMBERS, https://www.att.com/Common/about_us/pdf/att_btn.pdf (last visited Oct. 20, 2014).

sponded to Senator Markey's investigation reported retaining the information for periods including six months,[85] a year,[86] and eighteen months.[87]

There are plenty of non law-enforcement reasons why wireless providers would want to keep historical records of this activity—billing purposes,[88] tracking changes in network usage,[89] and consumer research to allow wireless providers to better serve their customers[90] are all plausible, acknowledged, and legitimate reasons to collect this data.[91] Cellular phone companies have been hesitant to enumerate the specific reasons for collecting such data besides the vague generalities contained in their privacy policies.[92] Cities in Europe have used this data to study the flow of people and cars in cities in order to better understand the patterns of daily life and make city services more effective.[93] Additionally, there are lucrative commercial reasons for storing such data, as it is invaluable to marketers and companies seeking to profit off insights on people's daily habits.[94] In sum, though the reasons for collecting the data are not entirely clear, there exist a host of plausible explanations in no way connected to law enforcement.

85. *See* Letter from Robert J. Irving, Jr. to Representative Edward Markey, *supra* note 54 (Leap Wireless/Cricket Communications); Letter from Tony Russo to Senator Edward Markey, *supra* note 54 (T-Mobile).

86. *See* Letter from John C. Gockley to Senator Edward Markey, *supra* note 54 (U.S. Cellular); Letter from William B. Petersen to Senator Edward Markey, *supra* note 56 (Verizon).

87. *See* Letter from Benjamin Moncrief to Senator Edward Markey, *supra* note 55 (C Spire Wireless).

88. O'Malley, *supra* note 25, at 22–23.

89. *Questions About Location Information*, AT&T, https://www.att.com/Common/about_us/privacy_policy/print_policy.html#location (last visited Oct. 21, 2014) ("We monitor, collect and use wireless location information, together with other information we get from our network and your wireless device, to maintain and improve our network.").

90. *Id.* ("We also might use location information with your consent to provide you with a customized experience.").

91. *See Blaze Testimony*, *supra* note 47, at 58 ("Creating and maintaining detailed records about the locations of phones as they move from place to place makes good engineering sense . . . . Such information will be collected because it is extraordinarily valuable for network management, for marketing, and for developing new services.").

92. Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, http://www.nytimes.com/2011/03/26/business/media/26privacy.html ("Verizon, for example, declined to elaborate [on why it retains cellular location information] other than to point to its privacy policy . . . ."); *see, e.g.*, *Sprint Corporation Privacy Policy*, SPRINT, http://www.sprint.com/legal/privacy.html#personal (last updated May 2, 2014) ("We use your personal information for a variety of purposes, including providing you with Services. We use your personal information to do things like: . . . Anonymize or aggregate personal information for various purposes like market analysis or traffic flow analysis and reporting. Monitor, evaluate or improve our products, Services, systems, or networks. Customize or personalize your experience with our Services. Customize or personalize online advertising to bring you information about products and services of Sprint or others that may interest you, including co-branded offers.").

93. *See* John Steenbruggen et al., *Mobile Phone Data from GSM Networks for Traffic Parameter and Urban Spatial Pattern Assessment: A Review of Applications and Opportunities*, 78 GEOJOURNAL 223, 235–36 (2013) (discussing projects in Rome and Amsterdam).

94. *Questions About Location Information*, *supra* note 89 ("We use [location information] for [a]dvertising."); *see also* Cohen, *supra* note 92 (stating that "the information . . . could be lucrative for marketers").

### *B. How Is Historical Location Data Obtained by Law Enforcement?*

Compelled disclosure of historical location data is governed by the SCA.[95] Historical location data is a noncontent electronic communication under the definition of the SCA,[96] meaning it can be obtained at the command of a court order under the SCA.[97] Specifically, Section 2703(d) of Title 18 of the U.S. Code provides that any "court of competent jurisdiction" can issue such a court order when a "governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[98] The "specific and articulable facts" language, of course, seems to borrow from the standard for an investigative detention under *Terry v. Ohio*.[99] As to what this standard means, the Court has elaborated that where "probable cause means a fair probability that contraband or evidence of a crime will be found,"[100] then the specific and articulable facts standard "is obviously less demanding."[101] The Court has cautioned that while reasonable suspicion is not an "inchoate and unparticularized suspicion or hunch"[102] and requires "some minimal level of objective justification for making the stop,"[103] nevertheless the

95. Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1860 (codified at 18 U.S.C. §§ 2701–12 (2012)). The term "Stored Communications Act" has become a popular shorthand term for this portion of the Electronic Communications Privacy Act and this Note has used and will use this convention. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 & n.1 (2004) [hereinafter Kerr, *User's Guide*].

96. 18 U.S.C. § 2703(c) (2012); *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, 306 (3d Cir. 2010).

97. § 2703(d).

98. *Id.* There currently exists a circuit split with regards to a portion of the legal standard under section 2703(d). The Third Circuit held in 2010 that a judge evaluating an application for a court order has the discretion, under the language of the statute, to require that the government apply for a warrant—in other words, rise to a probable cause standard—even for "non-content" information. *See In re U.S. for an Order*, 620 F.3d at 319 ("Because the statute as presently written gives the [judge] the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly because Congress also included the option of a § 2703(d) order."). The Fifth Circuit has held, however, that section 2703(d) is not discretionary and a judge "shall issue" a court order compelling the disclosure if the government rises to the "specific and articulable facts" standard in section 2703(d). *See In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 607 (5th Cir. 2013) ("If [the] conditions [of 18 U.S.C. § 2703(d)] are met, the court does not have the discretion to refuse to grant the order.").

99. 392 U.S. 1, 21 (1968) ("And in justifying the particular intrusion [in this case, a warrantless investigatory detention] the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion [by showing a crime may be afoot].").

100. United States v. Sokolow, 490 U.S. 1, 7 (1989) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)) (internal quotation marks omitted).

101. *Id.*

102. *Id.* (quoting Terry v. Ohio, 392 U.S. 1, 27 (1968)) (internal quotation marks omitted).

103. *Id.* (quoting INS v. Delgado, 466 U.S. 210, 217 (1984)) (internal quotation marks omitted).

concept is not "readily, or even usefully, reduced to a neat set of legal rules."[104]

What sort of "specific and articulable" facts has the government marshaled in order to receive cellular location information? In requesting the cellular location information for Antoine Jones' phone, the section 2703(d) application stated that the government was "conducting a criminal investigation of the user[] of the target cellular telephone identified above . . . . Based upon reliable information, it is believed that the user[] . . . utilizes the target cellular telephone in furtherance of . . . a conspiracy to distribute and to possess with intent to distribute narcotic controlled substances."[105] This minimalist statement was all that was necessary to obtain sixty days of cellular location information for Jones' phone. On its face, it seems that this statement might implicate the concerns analogous to those of *Nathanson v. United States*,[106] where the Supreme Court held that a search warrant could not issue "upon mere affirmance of suspicion or belief without disclosure of supporting facts or circumstances."[107] The statements in the above *Jones* affidavit are general, conclusory beliefs about Jones' criminal activity. To the extent they constitute specific and articulable facts, they disclose that Jones is the target of an ongoing criminal investigation and that the investigation indicates that Jones uses a cellular phone in connection with dealing drugs. In seeking to suppress the historical cellular location information, Jones advanced this argument to the district court.[108] The SCA, however, provides no statutory suppression remedy,[109] and, therefore, the district court noted, "assuming the applications lacked sufficient factual support, the [c]ourt would be powerless to order the suppression of the evidence that the government had obtained."[110]

This demonstrates another consequence of the distinction between a standard calling for only "specific and articulable facts" under the SCA and a standard calling for a showing of probable cause under the Fourth Amendment. A constitutional standard would provide a constitutional

104. *Id.* (quoting Illinois v. Gates, 462 U.S. at 232) (internal quotation marks omitted); *see also* Navarette v. California, 134 S. Ct. 1683, 1687 (2014) (stating that the reasonable suspicion "standard takes into account the totality of the circumstances—the whole picture") (internal quotation marks omitted).

105. Opposition to Motion to Suppress Cell Site Data, Ex. 2. ¶ 2, United States v. Jones, 908 F. Supp. 2d 203 (D.D.C. 2012). Though the government alleged the user to be Antoine Jones, in fact, as the government acknowledged in its application, the wireless subscriber was a person named Denise Jones. *See id.*

106. 290 U.S. 41 (1933).

107. *Id.* at 47.

108. United States v. Jones, 908 F. Supp. 2d 203, 209 (D.D.C. 2012) (describing Jones' "second statutory claim—that the applications did not contain sufficient 'specific and articulable facts' to support the court orders").

109. *See* 18 U.S.C. § 2708 (2012) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); *see also* Kerr, *User's Guide*, *supra* note 95, at 1224 (noting the absence of a statutory suppression remedy in the SCA).

110. *Jones*, 908 F. Supp. 2d at 209.

suppression remedy.[111] Short of that, in the law as currently constituted, an arguably conclusory affidavit such as that provided to gain sixty days of historical cellular location information in the *Jones* case cannot be addressed after it is has been signed by the initial judicial officer.[112]

This does not suggest that the government routinely files general and conclusory affidavits. In fact, in many instances the government provides a wealth of specific and articulable facts to justify their application for access to historical cellular location information. For instance, for several years law enforcement investigated Ronald Herron, a leader of the "Murderous Mad Dogs" set of the Bloods street gang, for running a violent, drug-dealing operation in the Gowanus Houses, a public housing community in Brooklyn.[113] In 2009, prosecutors requested well over a month of historical cellular location information for a telephone owned by Herron.[114] In support, an Assistant United States Attorney discussed information regarding Herron's drug dealing "established" by the investigation from a diverse group of sources, including "information provided by numerous undercover police officers who have successfully purchased narcotics from co-conspirators, other confidential sources, and a cooperating witness who personally distributed narcotics for [Herron]."[115] Therefore, while the possibility that a generally conclusory court order may be approved by a judicial officer and not allow for any suppression down the line, there is no evidence this is a prevalent problem.

### *C. How Is Historical Location Data Used in Criminal Investigations?*

The use of cellular location data in the *Jones* and *Machado-Erazo* cases offer examples of how cellular location data is used in the eventual prosecution of a crime. Cellular location data, however, can be used solely for the investigation of a crime.[116] In these early stages, the information

111. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("We hold that all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court."); Weeks v. United States, 232 U.S. 383 (1914) (holding that evidence obtained by the government in violation of the Fourth Amendment is not admissible in federal court).

112. *See Jones*, 908 F. Supp. 2d at 209; *see also* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("The statute specifically allows for civil damages and criminal punishment for violations of the ECPA, but speaks nothing about the suppression of information in a court proceeding.") (citations omitted).

113. Press Release, U.S. Att'y's Office, E. Dist. of N.Y., Leader of Bloods Street Gang Indicted for Racketeering, Including Three Murders and Three Attempted Murders (Feb. 13, 2012), *available at* http://www.fbi.gov/newyork/press-releases/2012/leader-of-bloods-street-gang-indicted-for-racketeering-including-three-murders-and-three-attempted-murders.

114. Sealed Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info. at 4, United States v. Herron, 2 F. Supp. 3d 391 (E.D.N.Y. 2014) [hereinafter Sealed Application of the U.S.].

115. *Id.* at 3.

116. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 4 (2011) (statement of James A. Baker, Associate Deputy Attorney General), *available at* http://www.judiciary.senate.gov/imo/media/doc/11-4-6%20Baker%20Testimony.pdf [hereinafter *Baker Testimony*] ("[N]on-

"is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity."[117] It can also provide other types of investigative leads, including the location of evidence or the meeting place of coconspirators.[118] Additionally, cellular location information "gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant."[119]

As a general rule, cellular location data can yield some of the same results as physical surveillance.[120] This can be especially useful for law enforcement when they lack the resources to follow or detain every person at a particular location during an investigation.[121] For example, in January 2012, the Federal Bureau of Investigation ("FBI") was investigating a cross-country marijuana trafficking organization involving a Massachusetts man named John Kosta.[122] As part of this investigation, law enforcement used cellular location information to supplement and buttress physical surveillance. For instance, after obtaining information that the leader of the marijuana trafficking organization was traveling from Arizona to Massachusetts, law enforcement first used cellular location information to locate the man in a mall parking lot.[123] There they observed the man and others with him transfer large black duffle bags from one car to another.[124] At one point, one of the men opened one of the duffle bags and pulled out a large amount of money.[125] When the vehicles left, investigators followed them as far as the Connecticut state line, but based on their cellular location information, were able to ascertain that they drove back to Arizona.[126]

Later in the investigation, John Kosta and several associates traveled to Arizona from Massachusetts.[127] They subsequently left Arizona in

content information [such as cellular location information] may be equally important, particularly at the early stages of a criminal or national security investigation.").

117. *Id.*

118. Sealed Application of the U.S., *supra* note 114, at 2–3 (describing how the historical cellular location information sought in the case "will further the investigation by . . . providing leads as to subjects' residences and meetings, and location of evidence").

119. *Baker Testimony*, *supra* note 116, at 4.

120. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 408 (1997) (noting that technologically-assisted physical surveillance might prove superior because it may be a "more reliable, less expensive, safer, and less intrusive . . . means of conducting surveillance").

121. *See id.* (noting, in the context of the beeper tracking devices, that "[b]eepers can track a target for prolonged periods, saving human capital and decreasing physical danger").

122. United States v. Kosta, No. 12-10226, 2013 WL 5934030, at *1–3 (D. Mass. Oct. 31, 2013).

123. Assented-To Motion to Late File Government's Global Opposition to Defendant John Kosta's Motion to Supress [sic] Evidence and Motion to Sever, Ex. 1 (Affidavit of Stephen J. Kelleher in Support of Search Warrant), at ¶ 11, United States v. Kosta, No. 12-10226, 2013 WL 5934030 (D. Mass. Oct. 31, 2013) [hereinafter Kelleher Affidavit].

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.* ¶ 18.

a three-car caravan.[128] After developing independent probable cause, a South Dakota state trooper stopped one of the vehicles and located 980 pounds of marijuana.[129] Kosta was not driving that car, but cellular location information indicated that "one of John Kosta's phones was traveling eastbound toward Massachusetts between January 6–8, 2012."[130] This information, along with the mall parking lot meeting and trip back to Arizona, served as a partial basis for an affidavit in support of a search warrant for Kosta's Massachusetts residence.[131] The search recovered "103 marijuana plants, 25 firearms, . . . [and] body armor."[132] It should be noted that, unlike *United States v. Jones*, discussed in the Introduction, the cellular location evidence would likely not have been necessary to establish links between Kosta and the Massachusetts residence because it appears settled that it was Kosta's residence.[133]

Cellular location data can also be used to focus on or exclude suspects early in an investigation. While investigating the murder of a young woman discovered "wrapped in plastic and partially decomposed" near the Longfellow Bridge in Malden, Massachusetts,[134] state police investigators began to focus on her boyfriend, Shabazz Augustine, as a possible suspect.[135] A month after the woman's body was discovered, state police investigators and the Middlesex County District Attorney's Office used an order issued under section 2703(d) to compel fourteen days of location data that Sprint had for Augustine's phone.[136] The stated purpose of this data—which totaled sixty-four pages—was to "show the general location of the defendant and [the victim] on August 24 and 25 to possibly include or exclude the defendant as a suspect."[137]

Cellular location information may also be able to locate wanted suspects and other physical evidence. After an East Baton Rouge Deputy Sheriff was shot in the neck in April 2010, investigators were able to obtain an arrest warrant for attempted first-degree murder of a police officer.[138] Investigators then "used . . . subpoenas and court orders to the

128. *Id.* ¶ 19.
129. *Id.* ¶ 20.
130. *Id.* ¶ 21.
131. United States v. Kosta, No. 12-10226, 2013 WL 5934030, at *3 (D. Mass. Oct. 31, 2013).
132. *Id.* at *4. The search warrant was later found to be invalid based on staleness. *See id.* at *5–7.
133. *See id.* at *1 (referring to the Phillipston house as the "Kostas' residence"). Of course, this decision was rendered in response to a motion to suppress, and, therefore, Kosta may have reserved the argument that he could not be adequately linked to the house or drugs inside for a trial on the merits. *See also* George Barnes, *FBI, Police Raid Phillipston Home over Federal Drug Charges*, TELEGRAM.COM (Aug. 9, 2012), http://www.telegram.com/article/20120809/NEWS/108099878/0 ("Phillipston Police Chief Kevin Dodge said the house has been the source of local speculation as the walls went up around it since it was bought by the Kostas in 2005.").
134. Mac Daniel, *Body Recovered from Charles Confirmed as Missing Woman's: DA's Office Sees Signs of Murder*, BOS. GLOBE, Sept. 21, 2004, http://www.boston.com/news/local/articles/2004/09/21/body_recovered_from_charles_confirmed_as_missing_womans/. The woman's car had been found a month earlier after being set on fire with her keys and cellular phone inside. *Id.*
135. Commonwealth v. Augustine, 4 N.E.3d 846, 850–51 (Mass. 2014).
136. *Id.* at 850.
137. *Id.* at 850–51 (internal quotation marks omitted).
138. *Baker Testimony*, *supra* note 116, at 4.

cell phone companies to obtain the suspect's calling records and location records. This information ultimately allowed officers to confirm the suspect's location."[139] In addition to providing weighty trial testimony, the cellular location information also operates in the background, underlying investigations and informing the basis for search and arrest warrants.

### *D. How Is Historical Cellular Location Information Presented in Court?*

"In a criminal jury trial, establishing a defendant's location during the commission of the crimes charged" is among "the most important factors . . . to the jury's determination of whether a defendant is guilty of those crimes."[140] Traditional methods of establishing this location—eyewitness testimony, physical evidence linking the defendant to the crime scene, or footage from surveillance cameras—remain the most common and influential methods of proving location.[141] "[T]raditional defendant location evidence," however, is "supplemented with historical cell site analysis . . . evidence in cases where one or more cellular phones can be connected to defendants, co-conspirators, accomplices, victims, or witnesses at times and places relevant to the charged offenses."[142]

*Machado-Erazo* and *Jones* are instructive in this regard. In both cases, the evidence was used to supplement large amounts of traditional evidence indicative of guilt. Though in *Jones* the evidence seemed to occupy a more important and central space in the prosecution's case after the suppression of the GPS tracking information, the prosecution still had information from surveillance, informants, text messages, and a Title III wiretap.[143] A review of reported decisions reveals few cases in which this evidence forms such an important part of the trial that it can be seen

139. *Id.* The suspect, DeWayne Steward, subsequently killed himself after police surrounded the location where he was hiding. David J. Mitchell & Katie Kennedy, *Shooting Suspect Dies in Darrow Standoff*, ADVOCATE (Baton Rouge, La.), Apr. 10, 2010, *available at* NewsBank Record No. MERLIN_5098135.

140. O'Malley, *supra* note 25, at 16.

141. *Id.* at 16; *see also* Mark L. Krotoski, *Effectively Using Electronic Evidence Before and at Trail*, 59 U.S. ATT'Y'S BULL. 52, 58 (2011).

142. O'Malley, *supra* note 25, at 16. This Note will not discuss the controversy over admissibility regarding this cellular location information, but it observes that defendants are increasingly challenging the admission of this evidence under provisions of the Federal Rules of Evidence and the reliability demands of *Daubert v. Merrel Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). *Compare* United States v. Davis, No. 11-60285, 2013 WL 2156659, at *7 (S.D. Fla. May 17, 2013) (turning aside a defendant's challenge to the reliability of cellular location data testimony, stating, "the Government has adequately demonstrated the reliability of [cellular location] methodology to satisfy *Daubert*'s reliability prong"), *with* United States v. Evans, 892 F. Supp. 2d 949, 957 (N.D. Ill. 2012) (excluding certain, but not all, cellular phone location data after finding its ability to locate a person with a certain area to not satisfy reliability under *Daubert*), *and* Michael Cherry et al., *Cell Tower Junk Science*, 95 JUDICATURE 151, 151 (2012) (describing how despite government-mandated ability to locate all phones through cell tower triangulation or GPS, "[i]nexplicably, at many criminal trials the prosecution uses a different approach," which is far less accurate).

143. United States v. Jones, 451 F. Supp. 2d 71, 74, 79 (D.D.C. 2006); *see also infra* notes 451–52 and accompanying text.

as crucial or evidence upon which the case hinges.[144] In fact, courts have noted this fact in motions for a new trial or on appeal, stating that even if the cellular location data were to be suppressed, it would not have affected the outcome of the trial.[145] For instance, in the Missouri case of *State v. Patton*, location data cast doubt on Melvin Patton's alibi that he was sleeping at his cousin's house in Cahokia, Illinois, instead of committing a double-murder in St. Louis.[146] The Missouri Court of Appeals, however, stated,

> Even without those records . . . the State presented overwhelming evidence that Patton was not only at the crime scene, but also the shooter. Two eye witnesses, one of the shooting victims and Patton's own son, identified Patton as the gunman. Also, Patton's cellmate testified that Patton confessed the shootings to him.[147]

There are, however, cases where the cellular location data plays an outsized role. At least one category of these cases is where cellular location data is used as corroboration evidence for accomplice testimony. For instance, the Texas Code of Criminal Procedure states that a person cannot be convicted of an offense "upon the testimony of an accomplice unless corroborated by other evidence tending to connect the defendant with the offense committed."[148] When Quintin Fisher was convicted of capital murder in 2011, however, the corroborating testimony consisted of "cell phone records, testimony regarding the location of the cell towers being accessed by the parties' cell phones on the night of the murder" and the testimony of a witness who may have been asked to participate in the robbery that led to the murder.[149] The appeals court judged this to be sufficient to corroborate the accomplice testimony.[150] The presentation of cellular location testimony, therefore, is most often done in circumstances where the testimony buttresses and supplements cases; sometimes, though, this evidence is called upon to shoulder a heavy load in circumstances when corroborating evidence is difficult to obtain.

### *E. What Supreme Court and Fourth Amendment Case Law Applies to It?*

The Fourth Amendment declares,

> 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

144. O'Malley, *supra* note 25, at 16 (stating that "eyewitness testimony and physical evidence" are the "primary methods of proving a defendant's location at times and places relevant to the charged offenses," but that the information "may be supplemented" with cellular location information).
145. *See, e.g.*, State v. Patton, 419 S.W.3d 125, 133 (Mo. Ct. App. 2013).
146. *Id.* at 128–29, 132.
147. *Id.* at 132.
148. TEX. CRIM. PROC. CODE ANN. art. 38.14 (West 2013).
149. Fisher v. State, No. 09-11-00379-CR, 2012 WL 5450828, at *8–12 (Tex. App. Nov. 7, 2012).
150. *Id.* at *12.

> cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[151]

Professor Wayne LaFave's opinion that these "fifty-four words . . . are not particularly illuminating" is even more true in the context of cellular phone technology.[152]

As an initial matter, the Fourth Amendment protects only against "unreasonable searches."[153] The Supreme Court has repeatedly held that the central touchstone of the Fourth Amendment is one of reasonableness.[154] "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[155] Generally, the Supreme Court has found that searches require a warrant,[156] though this requirement is "subject to certain reasonable exceptions,"[157] such as "special law enforcement needs, diminished expectations of privacy, [and] minimal intrusions,"[158] which create "general, or individual, circumstances [that] render a warrantless search . . . reasonable."[159]

This modern method of analyzing what is a search under the Fourth Amendment is derived from the test outlined in Justice Harlan's concurrence in *Katz v. United States*.[160] The test is two-pronged and asks first if the defendant "exhibited an actual (subjective) expectation of privacy," and second, whether "the expectation [is] . . . one that society is prepared to recognize as reasonable."[161] Katz had been convicted of using a telephone to take and place wagers.[162] During the investigation of Katz, law enforcement acted without a warrant in attaching "an electronic listening and recording device to the outside of the public telephone booth" that Katz used to place and take bets.[163] This allowed them to hear Katz's end of the telephone call without having to physically intrude on the booth.[164] At trial, the government introduced copies of the recordings in order to help secure Katz's conviction.[165] The majority opinion, authored by Justice Stewart, reversed the conviction, stating, "What a person knowingly exposes to the public, even in his own home or office, is not a sub-

151. U.S. CONST. amend. IV.

152. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A FOURTH AMENDMENT TREATISE ix (5th ed. 2012); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1974) ("For clarity and consistency, the law of the fourth amendment is not the Supreme Court's most successful product.").

153. U.S. CONST. amend. IV.

154. *See, e.g.*, Illinois v. McArthur, 531 U.S. 326, 330 (2001) (citing Texas v. Brown, 460 U.S. 730, 739 (1983)).

155. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

156. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

157. *Id.*

158. *McArthur*, 531 U.S. at 330.

159. *Id.*

160. 1 LAFAVE, *supra* note 152, 2.1(b), at 580.

161. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (internal quotation marks omitted).

162. *Id.* at 348 & n.1 (majority opinion).

163. *Id.* at 348.

164. *Id.*

165. *Id.*

ject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[166]

It was Justice Harlan's concurrence, however, with its two-prong "reasonable expectations" test, that has carried the day in Fourth Amendment jurisprudence.[167] Applying that test and defining its attributes, however, has been a struggle for the Court[168] and scholars[169] alike. This Note does not attempt to offer a "consistent explanation for what makes an expectation of privacy 'reasonable.'"[170] Instead, this Note will examine the Supreme Court's applications of this test in areas relevant to our inquiry on cellular phone location data. Among these are the tracking device cases of *United States v. Knotts*,[171] *United States v. Karo*,[172] and *United States v. Jones*;[173] the third-party doctrine cases, such as *United States v. Miller*[174] and *Smith v. Maryland*;[175] and lastly, *Kyllo v. United States*[176] and *Riley v. California*,[177] which, along with *Jones*, are paradigmatic examples of the Supreme Court's struggle to apply the Fourth Amendment in emerging technological contexts.

### *1. Tracking Cases*

The Supreme Court confronted its first case involving tracking in 1983. In *United States v. Knotts*, police in Minnesota investigating a methamphetamine-producing operation placed a tracking device called a "beeper" in a container of chloroform the suspects were going to purchase from a local chemical company.[178] Investigators used that beeper to

166. *Id.* at 351–52 (citations omitted).

167. RONALD JAY ALLEN, WILLIAM J. STUNTZ, JOSEPH L. HOFFMAN, DEBRA A. LIVINGSTON & ANDREW D. LEIPOLD, COMPREHENSIVE CRIMINAL PROCEDURE 368 (3d ed. 2011).

168. Oliver v. United States, 466 U.S. 170, 177–78 (1984) ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant. In assessing the degree to which a search infringes upon individual privacy, the Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.") (citations omitted).

169. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504–05 (2007) [hereinafter Kerr, *Four Models*] ("Although four decades have passed since Justice Harlan introduced the test in his concurrence in *Katz v. United States*, the meaning of the phrase 'reasonable expectation of privacy' remains remarkably opaque."); *see also* Amsterdam, *supra* note 152, at 385 ("In the end, the basis of the *Katz* decision seems to be that the fourth amendment protects those interests that may justifiably claim fourth amendment protection.").

170. Kerr, *Four Models*, *supra* note 169, at 503.

171. 460 U.S. 276 (1983).

172. 468 U.S. 705 (1984).

173. 132 S. Ct. 945 (2012).

174. 425 U.S. 435 (1976).

175. 442 U.S. 735 (1979).

176. 533 U.S. 27 (2001).

177. 134 S. Ct. 2473 (2014).

178. 460 U.S. 276, 278 (1983). A "beeper" is "[c]omparatively simplistic technology in today's hindsight," however, "such a beeper device emitted a radio-signal pulse at regular intervals and could only be followed manually by a police officer with a signal detector who stayed within signal range to

track a suspect during a long drive from Minneapolis to a clandestine methamphetamine laboratory in Shell Lake, Wisconsin.[179] At one point during the trip, the suspects began making "evasive maneuvers" and investigators ended their visual surveillance, but were able to keep tracking the suspects using the beeper.[180] Upon reaching the methamphetamine lab in Wisconsin, law enforcement applied for a search warrant and obtained one.[181] A search of the laboratory turned up enough precursor chemicals to produce fourteen pounds of methamphetamine.[182] The suspects moved to suppress the evidence seized from the lab because the warrant was the product of the warrantless beeper tracking.[183] The Court found no search violative of the Fourth Amendment to justify suppression by the Court.[184] The Court invoked the language of *Katz* and stated, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[185] The Court stated that no information was obtained by use of the tracker that could not have been obtained from "[v]isual surveillance from public places along [the] route or adjoining [the] premises."[186] These methods "would have sufficed to reveal all of these facts to the police" and thus the "fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [the] automobile to the police receiver" did not alter the court's analysis.[187] The end of the Court's opinion addressed arguments that allowing this sort of tracking would sanction the possibility of "twenty-four hour surveillance of any citizen . . . without judicial knowledge or supervision"[188] and that "bugged personal property . . . might push fortuitously and unreasonably into the private sphere protected by the Fourth Amendment."[189] To this, the Court stressed "the limited use which the government made" of the beeper tracking at issue, which was completely confined to one brief trip from Minneapolis to Wisconsin.[190] The Court, however, reserved a crucial question, stating, "[I]f such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[191]

avoid losing track of the device." Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), the Fourth Amendment "GPS Case,"* 65 OKLA. L. REV. 491, 493–94 (2013).

179. *Knotts*, 460 U.S. at 278–79.
180. *Id.* at 278.
181. *Id.* at 279.
182. *Id.*
183. *Id.*
184. *Id.* at 285.
185. *Id.* at 281.
186. *Id.* at 282.
187. *Id.*
188. *Id.* at 283 (internal quotation marks omitted).
189. *Id.* at 284 (quoting United States v. Knotts, 662 F.2d 515, 518 (8th Cir. 1981)).
190. *Id.* at 284–85.
191. *Id.* at 284.

Just a year later, in *United States v. Karo*, the Supreme Court again confronted a case of beeper tracking.[192] Karo and his coconspirators were arrested after Drug Enforcement Administration ("DEA") agents installed a beeper in a container of ether that Karo had ordered.[193] The agents suspected that the ether would "be used to extract cocaine from clothing that had been imported into the United States."[194] Investigators used the beeper to track the container's travels from mid-September 1980 to mid-February 1981 before it finally ended up in a rental house in Taos, New Mexico.[195] Investigators "did not maintain tight surveillance" on the house "for fear of detection," but on two consecutive days, investigators used the beeper monitor to ascertain that the container of ether was still inside the house.[196] The next day, investigators applied for and received a warrant.[197] Execution of the warrant turned up cocaine and cocaine processing materials in the house, which the district court suppressed as the products of the warrantless beeper tracking.[198]

The Supreme Court distinguished *Karo* from *Knotts* by the fact that monitoring the beeper in the house in *Karo* allowed investigators to monitor property "that ha[d] been withdrawn from public view."[199] The Court found a Fourth Amendment violation where there was "monitoring of a beeper in a private residence, a location not open to visual surveillance."[200] This was because such monitoring "reveal[ed] a critical fact about the interior of the premises that the Government [was] extremely interested in knowing and that it could not have otherwise obtained without a warrant."[201] In *Knotts*, meanwhile, the Court concluded, "since the movements of the automobile and the arrival of the can containing the beeper in the area of the cabin could have been observed by the naked eye, no Fourth Amendment violation was committed by monitoring the beeper during the trip to the cabin."[202] This difference led to the Supreme Court holding that "[i]ndiscriminate monitoring of property that has been withdrawn from public view . . . present[s] far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight"[203] and required a warrant to monitor the beeper in a case implicating these interests.[204] Despite this holding, the Court reversed the Tenth Circuit and held that the evidence should not

192. 468 U.S. 705 (1984).
193. *Id.* at 708.
194. *Id.*
195. *Id.* at 708–10.
196. *Id.* at 709–10.
197. *Id.* at 710.
198. *Id.*
199. *Id.* at 715–16.
200. *Id.* at 714.
201. *Id.* at 715.
202. *Id.* at 713–14.
203. *Id.* at 716.
204. *Id.* at 718.

have been suppressed.[205] There was, the Court stated, sufficient probable cause to support a warrant because the investigators observed the ether being loaded into a truck, which they then tracked visually and by beeper as it traveled along public roadways and led them to the rental house.[206] Therefore, the Court stated, "it is clear that the warrant affidavit, after striking the facts about monitoring the beeper while it was in the Taos residence, contained sufficient untainted information to furnish probable cause for the issuance of the search warrant."[207]

Almost thirty years later, the Court confronted the evolution of the technology in *Karo* and *Knotts* in regard to Antoine Jones' Jeep Grand Cherokee in *United States v. Jones*.[208] During their investigation of Jones,[209] investigators applied for a warrant allowing them to attach a GPS device to Jones' car in order to track his movements.[210] The warrant authorized the GPS device to be attached within ten days in the District of Columbia.[211] Instead, investigators attached the device on the eleventh day while the car was in Maryland.[212] The GPS was active for twenty-eight days, generally establishing the location of Jones' car within 50 to 100 feet and producing over 2000 pages of data concerning the car's movements.[213] Before trial, unphased by the violation of the warrant issued, the United States maintained that use of such GPS tracking devices was not a search, did not require a warrant, and therefore almost all of the GPS evidence should be admitted.[214] Relying on *Knotts* and *Karo*, U.S. District Judge Ellen Segal Huvelle suppressed only the GPS tracking evidence that was obtained when Jones' car was parked inside the garage of his residence.[215]

On appeal to the U.S. Court of Appeals for the D.C. Circuit, the panel rejected the proposition that *Knotts* controlled this case and framed a broad question to be decided instead.[216] *Knotts* was a decision,

205. *Id.* at 719.
206. *Id.* at 719–21.
207. *Id.* at 721.
208. 132 S. Ct. 945, 948 (2012).
209. *See infra* Part I.
210. *Jones*, 132 S. Ct. at 948.
211. *Id.*
212. *Id.*
213. *Id.* The GPS device on Jones' car seems to have only generated data when the car was moving. Brief for the United States at 4, *Jones*, 132 S. Ct. 945 (No. 10-1259). The GPS device installed on Jones' car generally seemed to transmit time, date, latitude, and longitude, as well as an approximate address of the vehicle every ten seconds when the vehicle was moving. Brief for Respondent at 1–2, 14, *Jones*, 132 S. Ct. 945 (No. 10-1259). Reprinted here are three sample lines of data from GPS device installed on Jones' car:
09/27/05 11:59:12 local; 38°54'17"N 76°50'16"W; 2; MD: 9730 APOLLO DR, Lake Arbor, USA_MD
09/27/05 11:59:22 local; 38°54'16"N 76°50'17"W; 7; MD: 9740 APOLLO DR, Lake Arbor, USA_MD
09/27/05 11:59:32 local; 38°54'18"N 76°50'15"W; 14; MD: 9727 APOLLO DR, Lake Arbor, USA_MD.
*See* Defendant Jones' Supplemental Omnibus Pre-Trial Motion, Ex. 2, United States v. Jones, 451 F. Supp. 2d 71 (D.D.C. 2006) (No. 05-0386).
214. *Jones*, 451 F. Supp. 2d at 88.
215. *Id.*
216. United States v. Maynard, 615 F.3d 544, 556–58 (D.C. Cir. 2010).

the court wrote, concerned with the reasonable expectations of privacy of a person "traveling in an automobile on public thoroughfares . . . from one place to another."[217] The panel found that the case before them raised the issue that *Knotts* reserved: whether monitoring "movements 24 hours a day . . . as [a person] move[s] among scores of places, thereby discovering the totality and pattern of [their] movements from place to place to place" requires a warrant.[218]

Proceeding from this proposition, the court rejected the simple conclusion that because a person's movements occur largely in public spaces, they are "knowingly expose[d] to the public" and therefore not protected by the Fourth Amendment.[219] The court cautioned that the question to be asked was not whether it is physically possible for a person to be tracked around the clock in public spaces.[220] Instead, the proper question was whether a person reasonably expects to be tracked around the clock in public spaces.[221] Asking this question, the court found that the totality of those movements were "not actually exposed to the public" because the chance that "a stranger would observe all those movements is not just remote, it is essentially nil."[222] Nor were these movements "constructively exposed"; just because each individual movement occurred in public did not mean that the totality of Jones' movements were exposed to the public view.[223] Instead, the "whole" picture of a person's movements reveals much more—personal habits and generally an "intimate picture of . . . life"—than the individual movements themselves.[224] A person expects to be observed, for instance, traveling to church, work, or to participate in meetings or hobbies.[225] A person does not, the court argued, expect to be observed doing every single one of those things, thus developing a broad picture of a person's habits, contradictions, proclivities, flaws, and failings.[226] Therefore since a person's collective movements are neither actually nor constructively exposed to the public, a person subjectively expects privacy in those movements.[227]

The court then evaluated if Jones' expectation of privacy was reasonable. After evaluating state laws requiring a warrant for GPS tracking, decisions of courts that had decided the issue, and Supreme Court precedent that measured the reasonableness of police intrusions on per-

217. *Id.* at 557 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
218. *Id.* at 558.
219. *Id.* at 559 (quoting United States v. Katz, 389 U.S. 347, 351 (1967)).
220. *Id.*
221. *Id.*
222. *Id.* at 560.
223. *Id.* at 560–61.
224. *Id.* at 561–62.
225. *Id.* at 562–63.
226. *Id.* at 563 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain disconnected and anonymous." (internal quotation marks omitted)).
227. *Id.* at 563.

sonal privacy, the court arrived at the conclusion that the expectation of privacy Jones had in his movements was reasonable.[228] As Jones possessed a reasonable expectation of privacy in his movements over the course of a month, the court concluded, "the use of the GPS device to monitor those movements defeated that reasonable expectation."[229] A warrant was therefore required in order to engage in this sort of long-term GPS tracking, and, consequently, Jones' conviction was reversed.[230] The court's reasoning has been termed the "mosaic theory"[231] and has been widely viewed as groundbreaking in its full-throated articulation of a new Fourth Amendment principle.[232]

The Supreme Court unanimously affirmed the D.C. Circuit. Justice Scalia, writing for five members of the Court, however, found a Fourth Amendment violation based on the warrantless physical occupation of private property that occurred in placing a tracking device on the car.[233] The Court's opinion, in relying on a "trespass" rationale, did not need to consider reasonable expectations under *Katz* nor the "thorny problem[]" of whether tracking Jones "through electronic means, without an accompanying trespass, [was] an unconstitutional invasion of privacy."[234]

A concurrence, authored by Justice Alito and joined by Justices Ginsburg, Breyer, and Kagan, however, coalesced around the idea that Jones' "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[235] Justice Alito spent the majority of the concurrence critiquing the Court's property-based opinion, concluding that "it has little if any support in current Fourth Amendment case law . . . and . . . is highly artificial."[236] Justice Alito instead thought the case should be decided on the traditional *Katz* framework[237] and confronted the reasonable expectations of privacy in our new technological age.[238] Justice Alito specifically singled out cellular

228. *Id.* at 563–64.
229. *Id.* at 563.
230. *Id.* at 566–68.
231. This term, adopted widely by commentators and other courts, seems to come from a sentence in the opinion when discussing the "whole vs. parts" theory of constructive exposure: "As with the 'mosaic theory' often invoked by the Government in cases involving national security information, '[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.'" *Id.* at 562.
232. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) [hereinafter Kerr, *Mosaic Theory*] ("In *United States v. Maynard*, the D.C. Circuit introduced a different approach, which could be called a 'mosaic theory' of the Fourth Amendment." (footnote omitted)).
233. United States v. Jones, 132 S. Ct. 945, 949 (2012) ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").
234. *Id.* at 954.
235. *Id.* at 958 (Alito, J., concurring in the judgment).
236. *Id.*
237. *Id.* at 962.
238. *Id.*

phones as the "most significant"[239] of the technologies implicating Fourth Amendment concerns before concluding that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[240]

Justice Sotomayor, who joined the majority, penned a separate concurrence where she announced her agreement with Justice Alito that "longer term GPS monitoring in investigations impinges on expectations of privacy."[241] Justice Sotomayer then set her sights in particular on the third-party doctrine,[242] calling for its reconsideration, and saying that it "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[243] Instead, Justice Sotomayor announced that she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[244]

This trio of cases has left us with a disparate collection of rules. At the very least, short term tracking in public places requires no warrant. Tracking requires a warrant, however, if it reveals details of the home, such as the object or person's presence inside it. Lastly, a physical trespass to accomplish tracking will require a warrant on the theory that a physical occupation of space is a search. Most recently, however, in *United States v. Jones*, five justices seemed to agree that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[245] The implications of *Jones* outside of the narrow field of GPS tracking devices mounted to vehicles have been widely discussed and are unclear.[246] It has at the least given an avenue to advocates and

239. *Id.* at 963 ("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. For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking. . . . The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements." (footnote omitted)).

240. *Id.* at 964 (citations omitted).

241. *Id.* at 955 (Sotomayor, J., concurring) (internal quotation marks omitted).

242. *See infra* Part III.B.

243. *Jones*, 132 S. Ct. 8 at 957 (Sotomayor, J., concurring).

244. *Id.*

245. *Id.* at 955 (internal quotation marks omitted).

246. *See* Tom Goldstein, *Why* Jones *Is Still Less of a Pro-Privacy Decision than Most Thought (Conclusion Slightly Revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/; Orin Kerr, *Why* United States v. Jones *Is Subject to So Many Different Interpretations*, VOLOKH CONSPIRACY (Jan. 30, 2012, 4:59 PM), http://www.volokh.com/2012/01/30/why-united-states-v-jones-is-subject-to-so-many-different-interpretations/.

lower courts to question[247] and/or reject[248] traditional tracking case doctrine when dealing with new GPS technology.

### *2. Third-Party Doctrine*

Several courts have analyzed the problem of cellular location data under the infamous "third-party doctrine" of the Fourth Amendment. This doctrine is infamous because, as Professor Orin Kerr explains, the "verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong, but horribly wrong."[249] The basic idea behind the third-party doctrine is:

> [T]he 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.[250]

The Supreme Court developed the doctrine in *United States v. Miller*.[251] In *Miller*, Bureau of Alcohol, Tobacco, and Firearms agents investigating a suspected bootlegger obtained the suspect's bank account records by subpoenaing his banks.[252] The Court held that where Miller had voluntarily conveyed information to his bank regarding his account, he did not have Fourth Amendment protection.[253] The Court's opinion, authored by Justice Powell, stated that it was their duty to "examine the nature of the particular documents sought to be protected in order to determine whether there [was] a legitimate 'expectation of privacy' concerning their contents."[254] Here, where the documents "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"[255] Miller had "knowingly expose[d]" this information "to the public" and thus the information was "not a subject of Fourth Amendment protection."[256] The Court notably rejected the argument that because the bank was required by federal law

247. *See, e.g.*, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d) to Disclose Subscriber Info. and Cell Site Info., 849 F. Supp. 2d 177, 178 (D. Mass. 2012) (stating that the concurrences in *Jones* "raise questions").

248. *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (citing *Maynard* extensively in finding that probable cause must be supplied for cellular location information).

249. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009) [hereinafter Kerr, *Third Party*] (footnote omitted).

250. United States v. Miller, 425 U.S. 435, 443 (1976).

251. In his article, Professor Kerr traces the third-party doctrine back to what he calls "secret agent" cases of the 1950s and 1960s. Kerr, *Third Party*, *supra* note 249, at 567–69. Prior to the articulation in *Miller*, Professor Kerr points to *Couch v. United States*, 409 U.S. 322 (1973), as an early third-party doctrine case. *Id.* at 569.

252. *Miller*, 425 U.S. at 437–38.

253. *Id.* at 444.

254. *Id.* at 442.

255. *Id.*

256. *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)) (internal quotation marks omitted).

to maintain these records, the combination of this requirement and the ability to obtain these records by subpoena constituted an end run around the Fourth Amendment.[257]

Just three years later, the Court found that the analysis in *Miller* "dictate[d]" that a defendant could claim no legitimate expectation of privacy in phone numbers he dialed since he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[258] In *Smith v. Maryland*, the Court confronted the case of Michael Lee Smith. While investigating a robbery, police installed a pen register—a device that captures the outgoing numbers from a particular telephone line[259]—on Smith's phone without obtaining any legal process first.[260] The Court found first that Smith likely could not have entertained an actual expectation of privacy since he must have known that telephone numbers are conveyed to the phone company, and the phone company may make record of those numbers "for the purposes of checking billing operations, detecting fraud, and preventing violations of law."[261] Second, the Court found that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable" since "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[262]

### *3. New Technology Cases*

Though undoubtedly *Jones* could be termed a "new technology case," the Supreme Court has confronted several other cases recently that dealt explicitly with the effect of new technologies on the Fourth Amendment.

First among them is *Kyllo v. United States*.[263] In this case, agents of the U.S. Department of the Interior believed that marijuana was being grown in a particular house in Florence, Oregon.[264] Because indoor marijuana growth "requires high-intensity lamps," the agents decided to use a thermal imaging device to determine if an abnormal amount of heat was emanating from the home.[265] Indeed there was, which, in the investigator's experience, was indicative of an indoor marijuana growing operation.[266] Based partially on this information, investigators obtained a war-

257. *Id.* at 441–43.
258. Smith v. Maryland, 442 U.S. 735, 744 (1979).
259. *See* 1 LAFAVE, *supra* note 152, § 2.7(b), at 950 (quoting United States v. Caplan, 255 F. Supp. 805, 807 (E.D. Mich. 1966)) (defining what a pen register is).
260. *Smith*, 442 U.S. at 737.
261. *Id.* at 742 (quoting United States v. New York Tel. Co., 434 U.S. 159, 174–75 (1977)).
262. *Id.* at 743–44 (internal quotation marks omitted).
263. 533 U.S. 27 (2001).
264. *Id.* at 29.
265. *Id.*
266. *Id.* at 30.

rant that led to the discovery of a marijuana growing operation in the house.[267] Kyllo, the homeowner, was charged with manufacturing marijuana and moved to suppress the evidence.[268] After the district court refused to suppress and the Ninth Circuit affirmed, the Supreme Court considered the Fourth Amendment implications of a thermal imaging device.[269]

A thermal imaging device "detect[s] infrared radiation" and displays this information by "convert[ing] radiation into images based on relative warmth . . . somewhat like a video camera showing heat images."[270] The question the Court confronted was "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[271] The Court's analysis began with *Katz* and announced that despite potential difficulties in implementing the criteria of that decision, there was certainly a reasonable expectation of privacy inside the home.[272] Therefore, where details about the inside of the home—previously unknowable without physical intrusion—are obtained by use of "a device that is not in general public use," a search within the meaning of the Fourth Amendment has occurred.[273]

The Court in *Kyllo* also rejected a number of technical or mechanical definitions proposed by the government.[274] The government, for instance, contended that no physical intrusion of the home occurred where only heat emanating from the house was detected.[275] In response to this, the Court stated that "just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house."[276]

In other words, the court's conception of physical intrusions of the home did not turn on *actual* physical intrusions. The Court declined to

> leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule . . . adopt[ed] must take account of more sophisticated systems that are already in use or in development.[277]

Furthermore, where the government attempted to argue that the "intimate details" of the home were not exposed by the technology, the Court

267. *Id.*
268. *Id.*
269. *Id.* at 30–31.
270. *Id.* at 29–30.
271. *Id.* at 34.
272. *Id.*
273. *Id.* at 40.
274. *Id.* at 35–37.
275. *Id.* at 35.
276. *Id.*
277. *Id.* at 35–36.

rejected this attempt to tie the Fourth Amendment's protections to the "quality or quantity of information obtained."[278]

Professor LaFave has cheered this decision on two grounds. First, it "is true to the teaching of *Katz* that what is most important is whether there has been an intrusion upon a justified expectation of privacy, and not . . . whether there had been a physical intrusion into some protected area."[279] Second, "is the Court's forthright recognition of the need to take a stand *now* against the increasing intrusiveness of modern technology, instead of waiting . . . until the equipment is even more sophisticated and the intrusions even more severe."[280]

Finally, and of special relevance, is the Court's recent decision in *Riley v. California*.[281] This case marks the first time the Court considered the Fourth Amendment implications of the capabilities and salience of cellular phones in modern society.[282] *Riley* concerned a pair of cases where police had searched a cellular phone incident to arrest.[283] In one case, police in San Diego arrested David Riley for driving on a suspended license.[284] David Riley's smart phone was in his pants pocket when he was arrested and the arresting officer looked through it and saw evidence of membership in the Bloods street gang.[285] Back at the police station, that officer turned the phone over to a gang detective, who examined its contents further and located more evidence (photographs and videos) of gang membership.[286] The detective also found evidence connecting Riley to a shooting a few weeks earlier.[287] When Riley was brought to trial on charges relating to the shooting, he sought to suppress the testimony about the phone's contents, as well as photographs the state intended to introduce into evidence.[288] The court denied his motion, and he was convicted and sentenced to fifteen years in prison.[289]

In the companion case, police in Boston witnessed Brima Wurie do a drug deal.[290] They arrested him and searched his phone incident to arrest.[291] Using information they gathered from the phone, they located

278. *Id.* at 37.
279. 1 LAFAVE, *supra* note 152, § 2.2(e), at 654.
280. *Id.* at 655.
281. 134 S. Ct. 2473 (2014).
282. *See City of Ontario v. Quon*, 560 U.S. 746, 755–59 (2010). In *Quon*, the Court considered whether a search of a government employee's messages on a government-issued pager violated the Fourth Amendment. *Id.* at 750. The Court recognized that it was dealing with issues of "far-reaching significance" but utilized "settled principles" to decide the case, *id.*, writing, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Id.* at 759.
283. *Riley*, 134 S. Ct. at 2480.
284. People v. Riley, No. D059840, 2013 WL 475242, at *2 (Cal. Ct. App. Feb. 8, 2013).
285. *Riley*, 134 S. Ct. at 2480.
286. *Id.* at 2480–81.
287. *Id.* at 2481.
288. *Id.*
289. *Id.*
290. *Id.*
291. *Id.*

Wurie's apartment.[292] They returned to the apartment a short time later with a search warrant and located "215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash."[293]

In a unanimous decision authored by Chief Justice Roberts, the Supreme Court found that the search incident to arrest doctrine did not apply to a cellular phone located on a person.[294] Unlike in the historical cellular location information cases, there was no question that the cellular phone had been subjected to a search,[295] so the court began by considering the "reasonableness" of searching the phone without a warrant, balancing the governmental intrusion on individual privacy against the governmental interest in searching without a warrant.[296]

The Court considered the relevant precedent[297] on the search incident to arrest doctrine, finding that the government's interests in officer safety and evidence destruction—which have traditionally supported warrantless searches incident to arrest—were not served by searching through the data contents of a cellular phone.[298]

The Court then turned to considering the balancing concern of individual privacy interests. In one of the decision's more memorable passages, the Court found that comparing the search of a person's pockets and its contents (a cigarette pack is the paradigmatic example from the case law[299]) to the search of cellular phone's contents "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[300] The Court then enumerated a host of increased privacy concerns in a cellular phone's contents, including the aggregation of diverse bits of data, which serves to "reveal much more in combination than any isolated record."[301] Furthermore, the contents are comprehensive, detailed, and often are a complete record dating to the purchase of the phone.[302] The Court's opinion also stated, however, that though

> the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. . . . Data on a cell phone can . . . reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements

292. *Id.*
293. *Id.*
294. *Id.* at 2485.
295. *Id.* at 2492–93.
296. *Id.* at 2484.
297. *See* Arizona v. Gant, 556 U.S. 332 (2009); United States v. Robinson, 414 U.S. 218 (1973); Chimel v. California, 395 U.S. 752 (1969).
298. *See Riley*, 134 S. Ct. at 2485–88.
299. *See Robinson*, 414 U.S. at 223.
300. *Riley*, 134 S. Ct. at 2488.
301. *Id.* at 2489.
302. *See id.* at 2489–90.

> down to the minute, not only around town but also within a particular building.[303]

Thus the Court found that the balance between government interests and individual privacy weighed very heavily in favor of the latter concern.[304] The Court concluded with a tour through the revolutionary underpinnings of the Fourth Amendment—its protection against general warrants and writs of assistance—before providing the "answer to the question of what police must do before searching a cell phone seized incident to an arrest . . . [:] get a warrant."[305]

## III. ANALYSIS

Faced with a rapidly evolving technological landscape and a confusing morass of new, unsettled case law (*Jones* and *Riley*) and thirty-year-old precedent (*Miller*, *Smith*, *Knotts*, and *Karo*), it is unsurprising that courts have come to a host of different conclusions about how best to confront historical cellular location information.

These courts have generally approached the cellular location data cases from one of three angles. Some courts have used the third-party doctrine. Some courts applied the precedent from tracking cases. Other courts have analyzed on both grounds. Lastly, some courts have used the "mosaic theory" articulated in *Maynard* and made especially prominent by the concurrences in *Jones*. Courts have used all combinations of the available Supreme Court precedents, as well as influential lower court cases in order to justify the conclusions reached. This Part of the Note will analyze and comment on the major approaches taken by courts in analyzing historical cellular location information.

### *A. Third-Party Doctrine*

The leading case to approach cellular location data from a third-party doctrine perspective is *In re Application of the U.S. for Historical Cell Site Data*.[306] In this case, the Fifth Circuit overturned the decision of a federal magistrate judge who denied the government's *ex parte* application for a section 2703(d) court order holding that historical cellular location information required a warrant. Because of this, on the appeal, there

303. *Id.* at 2490 (citing United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

304. *See id.* at 2484–85.

305. *Id.* at 2494–95.

306. 724 F.3d 600 (5th Cir. 2013). The Fifth Circuit limited the holding in this case to applications to "obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call," and not, for instance, "orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods)." *Id.* at 615. It is unclear, given the court's reasoning, how the difference between an in-use and an idle phone would change the calculus.

was no party truly adverse to the government,[307] nor did the Fifth Circuit have the benefit of a true factual record, hearings, or expert testimony.[308] In considering the question, however, the Fifth Circuit panel held that "cell site information is clearly a business record" as "[t]he cell service provider collects and stores historical cell site data for its own business purposes."[309] The court found that these records were voluntarily conveyed in that they were sent to the provider "so that the provider can perform the service for which [the customer] pays it: to connect his call. . . . [H]istorical cell site information reveals his location information for addressing purposes, not the contents of his calls."[310]

The Fifth Circuit also found that cellular phone users know that part of what they communicate to their company is their location.[311] In order to use their cellular phone, users understand that their "phone must send a signal to a nearby cell tower in order to wirelessly connect [their] call."[312] If "they are out of the range of their service provider's network of towers" they will be unable to make calls.[313] This simple fact is reinforced, as another court recently recognized, by the ubiquity of cellular phone towers in many urban and suburban settings.[314] From this basic location concept, customers must necessarily realize that part of what is voluntarily communicated to wireless providers is information about that user's location.[315]

Even if that were not the case, the Fifth Circuit continued, "cell service providers' and subscribers' contractual terms of service and . . . privacy policies expressly state that a provider uses a subscriber's location

307. *Id.* at 602 ("Although there was no party adverse to the Government's ex parte application, the ACLU and Electronic Frontier Foundation ("EFF"), among others, participated as amici curiae.").

308. *See id.* at 602. Since this was an appeal from an *ex parte* application for a court order, there was no factual record or change to develop one. *Id.* The government's request for historical cell site data was denied by the magistrate judge, at which point the magistrate judge invited the government to brief its application for the data. *Id.* Four days after the Government submitted its brief, the magistrate judge issued a lengthy written opinion. *Id.* The Government appealed this decision to the district court, but, again, shortly after the submission of briefs (and apparently without benefit of oral argument or hearing), the district court denied the applications. *Id.* at 602–03.

309. *Id.* at 611.

310. *Id.* at 612.

311. *Id.* at 613.

312. *Id.*

313. *Id.*

314. *See* United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012) ("[I]t is nearly impossible to avoid regularly seeing cell towers in an urban area such as the Southern District of Florida. Thus . . . cell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers.").

315. *See Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613; *see also In re* Application of U.S. for an Order Authorizing Disclosure of Historical Cell Site Info. for Tel. No. [Redacted], No. 11-449, 2011 U.S. Dist. LEXIS 156744, at *15 (D.D.C. Oct. 3, 2011) ("[A] reasonable cellular phone customer presumably realizes that his calls are transmitted by nearby cell-site towers, and that cellular phone companies have access to and likely store data regarding the cell-site towers used to place a customer's calls.").

information to route his cell phone calls."[316] Additionally, courts have found that the "cell-phone-using public" is generally aware they can be billed for using their phone outside of their "home area."[317] In order to bill for this, often called "roaming" charges, cellular phone companies must collect and maintain certain types of information, including location information.[318] Since cellular phone users voluntarily use their phones despite this knowledge, courts have reasoned, they voluntarily convey the information and therefore fall within the third-party doctrine.[319]

In addition, a number of district courts have found that cellular location data is subject to the third-party doctrine.[320] A particularly influential district court articulation has been *United States v. Graham*.[321] In this prosecution, the government sought to connect two defendants with a series of fast-food restaurant robberies by showing—at least according to their historical cellular location information—that they were in the area of the robberies at the time the crimes occurred.[322] Graham challenged the historical cellular location data using a motion to suppress that recited a mosaic theory rationale.[323] He argued that the court order, which authorized the release of "two hundred and twenty-one days and 20,235 individual cell site location data points, infringed on [Graham's] expectations of privacy insofar as that data allows the government to paint an intimate picture of the Defendants' whereabouts over an extensive period of time."[324]

The court in *Graham* answered this argument with an extremely thorough examination of the issue before settling on the third-party doctrine as the appropriate avenue for resolving this case.[325] Like the Firth Circuit, the district court in *Graham* found that cellular location data "are the business records of the cellular providers."[326] Additionally, the

316. *Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613.

317. *Madison*, 2012 WL 3095357, at *8.

318. *Id.*

319. *See Application of the U.S. for Historical Cell Site Info.*, 724 F.3d at 613; *Madison*, 2012 WL 3095357, at *8.

320. *See, e.g.*, United States v. Banks, No. 13-CR-40060-DDC, 2014 WL 4594197, at *4 (D. Kan. Sept. 15, 2014); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d), No. M-50, 2014 WL 4388397, at *6 (S.D.N.Y. May 30, 2014); United States v. Salas, No. CR F 11-0354 LJO, 2013 WL 4459858, at *3 (E.D. Cal. Aug. 16, 2013); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *11–13 (D. Ariz. May 8, 2013); United States v. Wilson, No. 1:11-CR-53-TCB-ECS-3, 2013 WL 1129199, at *6 (N.D. Ga. Feb. 20, 2013); United States v. Ruby, No. 12 CR 1073 WQH, 2013 WL 544888, at *3–7 (S.D. Cal. Feb. 12, 2013); United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Md. 2012); United States v. Gordon, No. 09-153-02 (RMU), 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012); United States v. Suarez-Blanca, No. 07-CR-0023-MHS/AJB, 2008 WL 4200156, at *9 (N.D. Ga. Apr. 21, 2008).

321. *Graham*, 846 F. Supp. 2d 384. For an example of a case relying on *Graham*, see *Wilson* 2013 WL 1129199 (relying largely on *Graham*, *see infra*, in finding that third-party doctrine applies to cellular location information).

322. *Graham*, 846 F. Supp. 2d at 386.

323. *Id.* at 387.

324. *Id.*

325. *Id.* at 387–90.

326. *Id.* at 398 (internal quotation marks omitted).

court rejected a parallel argument that the cellular phone user has a property or ownership interest in the records, stating that they are "created and maintained by the cellular providers" and cellular phone users do not have access or the ability to turn them over in response to legal process.[327]

The *Graham* court found that "[l]ike the dialed telephone numbers in *Smith* [*v. Maryland*], the Defendants in this case voluntarily transmitted signals to cellular towers in order for their calls to be connected. The cellular provider then created internal records of that data for its own business purposes."[328] The court deftly turned the anachronistic technology from *Smith* on its head, pointing out that when *Smith* was decided, a pen register operated as a *de facto* tracking device.[329] At the time *Smith* was decided all phones were "land lines" and many of the land lines that had pen registers attached to them were inside spaces which implicate the Fourth Amendment—namely, homes and offices.[330] Therefore, the data collected by a pen register could establish location, in many cases much more precisely than the cellular location data at issue here.[331]

Ultimately, the court in *Graham* found the third-party doctrine to be compelling and the controlling law, holding, "[H]istorical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers."[332] Because "[d]efendants [had] no legitimate expectation of privacy in those records," the *Graham* court found no Fourth Amendment violation had occurred.[333]

There are a number of virtues to a third-party doctrine approach to the warrantless disclosure of historical cellular location information, and scholars have offered a robust defense of the third-party doctrine in this context.[334] First, the third-party doctrine is an easily understood bright-line rule. When you convey information to a third party, you lose your expectation of privacy in that information. This tracks other areas of Fourth Amendment inquiry. While the privacy of the home in Fourth Amendment jurisprudence is well established,[335] leaving the information and contents contained there exposed to third parties causes the reason-

327. *Id.*
328. *Id.* at 399.
329. *Id.*
330. *Id.*
331. *Id.*
332. *Id.* at 400.
333. *Id.* at 403.
334. *See, e.g.*, Orin Kerr, *Legal Protection for Historical Cell-Site Records,* VOLOKH CONSPIRACY (Feb. 3, 2010, 1:22 AM), http://www.volokh.com/2010/02/03/legal-protection-for-historical-cell-site-records/ [hereinafter Kerr, *Legal Protection*].
335. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

able expectation of privacy concerning that information to disappear.[336] Furthermore, if one invites a third party into their home, that person is free to go to the police and tell them about the things they heard or saw there.[337] There is, therefore, an intuitive and constitutional grounding to the doctrine.

For over forty years, society has accepted as reasonable the proposition in *Smith v. Maryland* that telephone numbers conveyed to a third party are not entitled to Fourth Amendment protection.[338] The historical cellular location information at issue here is an appropriate twenty-first century application of this doctrine. The Court found that in the time of *Smith v. Maryland* it was reasonable for people to understand that they necessarily conveyed numbers to the phone company in order to use the landline phone service and that the phone company retained a record of those numbers.[339] So too is it reasonable for modern cellular phone users to understand that they necessarily convey their location to the cellular phone company in order to use cellular phone service. Indeed, the ability of cellular phones to place and receive calls in almost any location is their *raison d'être*. And only a basic understanding of cellular phone technology is necessary to understand that location in regards to cellular phone towers is an essential part of this ability.[340] In fact, cellular phone compa-

336. *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that respondents had no reasonable expectation of privacy regarding the contents of trash bags left "at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so"); California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."); *see also* Georgia v. Randolph, 547 U.S. 103, 110 (2006) (stating that co-inhabitants "assume[] the risk that one of their number might permit the common area to be searched" (quoting United States v. Matlock, 415 U.S. 164, 171 n.7 (1974))).

337. *See* Hoffa v. United States, 385 U.S. 293, 301–03 (1966) (holding that there is no Fourth Amendment violation where an informant reports to the police on conversations overheard after being admitted to the defendant's hotel room); *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 518–19 (2011) [hereinafter Kerr, *Equilibrium Adjustment*] ("Imagine the police send an undercover agent into your home. You think the agent is a friend, so you let him in. He starts asking questions, and you tell him all sorts of private things on the assumption that he is a friend who will maintain your confidence. The agent then returns to police headquarters and tells everyone there about what you said. According to the Supreme Court, this scenario raises no Fourth Amendment issues at all."); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) ("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. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)). The consent-once-removed doctrine, recognized by several federal courts of appeal, is also something to consider in this context. *See* Pearson v. Callahan, 555 U.S. 223, 244–45 (2009) (citing cases approving the doctrine).

338. *See supra* notes 258–62 and accompanying text.

339. Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

340. *See* Kerr, *Legal Protection*, *supra* note 334.

nies frequently tout the breadth of their network coverage in advertisements, further driving home the point to consumers that your cellular phone company aims to locate you anywhere and everywhere you are.[341]

Furthermore, the rise of location-based services and applications for cellular phones has made the ability of the company to locate the user a desirable and necessary feature of cellular phones.[342] Today, adult smartphone owners comprise fifty-six percent of the total cellular phone users in the United States.[343] Moreover, "[n]early [sixty percent] of smartphone users employ apps that access their location data"[344] and seventy-four percent of adult smartphone users "use their phone to get directions or other information based on their current location."[345] Necessarily they must realize that their information is freely conveyed to the cellular phone company.

What ignorance might remain about this basic feature of cellular phone technology is decreasing at a rapid pace. One court cleverly noted that in 2005 the *New York Times*

> observed that "[m]ost Americans carry cellphones, but many may not know that government agencies can track their movements through the signals emanating from the handset." Last year, the *Times* dubbed such efforts by police as "a routine tool," observing that "the wide use of cell surveillance has seeped down to even small, rural police departments."[346]

In addition, recent disclosures of government surveillance programs have cast a bright light on the amount of information retained by cellular phone companies, further damaging any argument that cellular phone users, in general, do not understand that their information is stored.[347]

---

341. *See, e.g.*, *Why Verizon?*, VERIZON WIRELESS, http://www.verizonwireless.com/wcms/consumer/explore/why-verizon.html (last visited Oct. 24, 2014) ("Verizon's super-fast 4G LTE network is the most reliable and in more places than any other 4G LTE network. . . . [c]over[ing] over 97% of Americans."). Wireless companies frequently accompany these advertisements with full color maps displaying how much of America their network covers. *See id.* (displaying network coverage maps for Verizon, AT&T, Sprint, and T-Mobile).

342. Marcelo Ballve, *Beyond Check Ins: How Social Media Apps Are Driving a Boom in Location-Based Data*, BUS. INSIDER, (Sept. 26, 2013, 2:15 PM), http://www.businessinsider.com/social-media-boost-location-based-data-2013-9 (describing how "[l]ocation-based services will become ubiquitous" in mobile applications as consumers seek out applications with "location-sensitive features in the background").

343. MAEVE DUGGAN & AARON SMITH, PEW RESEARCH CTR., CELL INTERNET USE 2013 4 (2013), http://pewinternet.org/~/media//Files/Reports/2013/PIP_CellInternetUse2013.pdf.

344. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 141 (E.D.N.Y. 2013) (internal quotation marks omitted).

345. KATHRYN ZICKUHR, PEW RESEARCH CTR., LOCATION-BASED SERVICES 2 (2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Location-based%20services%202013.pdf.

346. *Smartphone Geolocation Data Application*, 977 F. Supp. 2d at 139.

347. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST, Dec. 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html ("The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents

Even some courts that have found historical cellular location information to require a warrant have not accepted the argument that cellular phone users are ignorant to the fact that their location information is conveyed to the wireless company, calling it a "doubtful proposition" that "cannot long be maintained."[348] To the extent that there are some cellular phone users who are ignorant as to how their cellular phone company knows when they are roaming versus communicating with their home network, it would be short-sighted indeed to advocate for a change in the third-party doctrine's framework as applied to cellular phones "on the incorrect understandings of a decreasing percentage of the population."[349]

Additionally, Professor Orin Kerr, a leading scholar of the Fourth Amendment, contends that the third-party doctrine is useful precisely because it reaches these types of new technological information.[350] His argument proceeds that "[j]ust as the Fourth Amendment should protect that which technology exposes, so should the Fourth Amendment permit access to that which technology hides."[351] Therefore, the third-party doctrine is essential to ensure the "technological neutrality" of the Fourth Amendment.[352] As criminals become more sophisticated and increasingly use technology to avoid law enforcement, the third-party doctrine ensures that technology does not combine with the Fourth Amendment to put these criminals completely out of reach. Without the third-party doctrine, cellular phones would act as impenetrable shields to law enforcement.

Some courts and commentators have criticized the reliance on the third-party doctrine in the historical cellular location information context.[353] Courts have instead found that cellular phone customers do not

and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals—and map their relationships—in ways that would have been previously unimaginable.").

348. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011).

349. *See* Kerr, *Legal Protection*, *supra* note 334.

350. *See* Kerr, *Third Party*, *supra* note 249, at 580–81 (2009).

351. *Id.* at 580.

352. *Id.* at 580–81.

353. *See, e.g.*, United States v. Herron, No. 10-CR-0615 (NGG), 2014 WL 824291, at *8–10 (E.D.N.Y. Mar. 3, 2014); *Application of the U.S. for Historical Cell-Site Info.*, 809 F. Supp. 2d at 120–22; *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578 (E.D.N.Y. 2010); *cf.* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (finding the National Security Agency's bulk telephone metadata collection program to not fall under the third-party doctrine because "[t]he question . . . is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, 'whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment,'—under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case. Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now") (internal citation omitted).

actually realize they are conveying their location information to the cellular phone companies.[354] As the Third Circuit has written, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way" since "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."[355] An influential decision from a magistrate judge in the Southern District of Texas contended, "[C]ell site data is neither tangible nor visible to a cell phone user."[356] "Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal. Thus . . . a cell phone user may well have no reason to suspect that her location was exposed to anyone."[357] The cases making these points, however, are already several years old. As has been demonstrated in the paragraphs above, these arguments grow less and less convincing by the day as smartphones with location-based capabilities have become the dominant cellular phone in the United States.[358]

In addition, many scholars have been sharply critical of the third-party doctrine.[359] In particular, they argue that it does not pass a basic test of common sense in many contexts. Professor LaFave and his colleagues have written that it is premised on "ownership" and "possession" of the records, which runs contrary to the declaration in *Katz* that "property concepts cannot 'serve as a talismanic solution to every Fourth Amendment problem.'"[360] Indeed, *Katz* added a privacy-based theory of the Fourth Amendment.[361] Therefore, it seems inapposite to find that the only legitimate interests in cellular phone records are those of the phone company, which has created them and has physical control of them.

The reasonable expectations of privacy that Justice Harlan discussed, the Court has recognized, must have "source[s] outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[362] The understandings, which have been recognized and permitted by society, these third-party doctrine critics argue, is that we share our personal information with a series of third parties, including cellular phone companies, which we deem "necessary to participate in ordinary

354. *See, e.g.*, *Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 844.

355. *In re* Application of the 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).

356. *Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 844.

357. *Id.*

358. DUGGAN & SMITH, *supra* note 343.

359. *See, e.g.*, Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1592 (2010).

360. WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 161 (5th ed. 2009) (quoting *Katz v. United States*, 389 U.S. 347, 351 n.9 (1967)).

361. United States v. Jones, 132 S. Ct. 945, 951 (2012) ("*Katz* . . . established that 'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property.'" (quoting Soldal v. Cook County, 506 U.S. 56, 64 (1992))).

362. Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978).

society."[363] It is not a logical conclusion that we then must assume the risk of sharing this information with the police, as the classic formulation of the third-party doctrine states. This rule produces a "narrow, individualistic conception of privacy that is deeply contrary to reality"[364] as "[m]uch of what is important in human life takes place in a situation of shared privacy."[365] Moreover, the services provided by these third parties are in many ways necessary to our modern Western existence[366] and, in particular, to participating and excelling in our society.[367] Information conveyed necessarily to participate in such a vital part of our society should not be deemed without any constitutional protection.[368]

Though the third-party doctrine has been the most popular and debated method for law enforcement to access historical cellular location information without a warrant, other courts have looked to the attributes of the information provided in formulating a Fourth Amendment rationale.

### *B. Tracking Cases*

"When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[369] This is the first sentence of the Sixth Circuit's recent consideration of cellular location information.[370] Melvin Skinner was a "courier" for James Michael "Mike" West.[371] Mike West, along with his brother Scott, were prominent developers and entrepreneurs who owned a host of popular businesses and restaurants in

363. Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 990 (2007).

364. RONALD JAY ALLEN ET AL., *supra* note 167, at 390.

365. *Id.* at 390 (quoting Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1593 (1987)).

366. DUGGAN & SMITH, *supra* note 343 (reporting that ninety-one percent of adults in the United States own a cell phone).

367. The government recognizes the essential value in having a cellular phone. The Federal Communications Commission sponsors a program called "Lifeline," which discounts cellular phone service for eligible low-income customers so that they may "connect to the nation's communications networks, find jobs, access health care services, connect with family and their children's schools, and call for help in an emergency." *Lifeline: Affordable Telephone Service for Income-Eligible Customers*, FED. COMMC'NS COMM'N, http://www.fcc.gov/guides/lifeline-and-link-affordable-telephone-service-income-eligible-consumers (last updated Apr. 8, 2014).

368. *See* LAFAVE ET AL., *supra* note 360, at 161–62 ("The proposition . . . that the Fourth Amendment will not come to the rescue of one who 'voluntarily confides his wrongdoing' to another is not applicable here [speaking of *Miller*], as for all practical purposes, the disclosure of one's financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without a bank account.").

369. United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).

370. *Id.* at 772, 774. Though this particular tracking occurred in the prospective/real-time cellular location information context, the Sixth Circuit's decision is analogous here.

371. *Id.* at 775.

downtown Knoxville, Tennessee.[372] It was mostly funded, however, by their primary business venture:[373] a large-scale multi-million dollar drug distribution organization, which transported marijuana from Arizona to Tennessee.[374]

In July 2006, through an informant, law enforcement investigators learned that Skinner, who at that time detectives only knew as "Big Foot," was making a trip from Tennessee to Arizona to pick up a load of marijuana.[375] Investigators discovered that Skinner was going to be using a "pay-as-you-go" phone to keep in contact while he transported the drugs, and they applied to a federal magistrate for an order "authorizing the phone company to release subscriber information, cell site information, GPS real-time location, and 'ping' data for . . . [that] phone in order to learn Big Foot's location while he was en route to deliver the drugs."[376]

After Skinner arrived in and left Arizona, based on the information gleaned from real-time location tracking, law enforcement stopped and arrested him near Abilene, Texas, in a motorhome containing over 1100 pounds of marijuana.[377] Skinner was charged and he "sought to suppress the search of the motorhome, alleging that the agents' use of GPS location information emitted from his cell phone was a warrantless search that violated the Fourth Amendment."[378] The magistrate judge and the district court rejected this argument, and Skinner was found guilty after a ten-day trial and sentenced to 235 months of imprisonment.[379]

The Sixth Circuit, ruling on Skinner's appeal, found that *Knotts* was the salient law, stating, "There is no inherent constitutional difference between trailing a defendant and tracking him via [new] technology. Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[380] Relying on a prior Sixth Circuit ruling, the court found that in Skinner's case "the cell-site data is simply a proxy for [the defendant's] visually observable location, and a defendant has no legitimate expectation of privacy in his movements along public highways."[381] Cognizant of the concurrences in *Jones*, the Sixth Circuit took pains to analogize Skinner's case to *Knotts* and stress the limited nature of the tracking at issue. Instead of the twenty-eight days in *Jones*, this tracking went on for

372. Jamie Satterfield, *Testimony Details West Drug Network, History*, KNOXVILLE NEWS SENTINEL, Jan. 28, 2009, http://www.knoxnews.com/news/2009/jan/28/testimony-details-west-drug-network-history/.

373. *Id.*

374. *Skinner*, 690 F.3d at 775.

375. *Id.* at 775–76.

376. *Id.*

377. *Id.* at 776.

378. *Id.*

379. *Id.* at 777.

380. *Id.* at 777–78.

381. *Id.* at 779 (quoting United States v. Forest, 355 F.3d 942, 951–52 (6th Cir. 2004)) (internal quotation marks omitted).

three days and encompassed one cross-country trip.[382] Therefore, the comprehensive tracking which lays bare the most intimate details of a person's life was not at issue there.

Certainly the third-party doctrine has been the most popular way to uphold the constitutionality of section 2703(d); the tracking cases, however, have been used as at least a fallback position.[383] Other courts and judges have adopted the tracking cases more openly and relied on them primarily.[384] For instance, the Third Circuit invoked this reasoning in holding that cellular location information does not always require a warrant.[385] Rejecting the premise that citizens possessed "reasonable expectations of privacy regarding their physical movements and locations," the Third Circuit stated that *Knotts* and *Karo* were the controlling opinions as they made clear that the privacy interests involved in tracking were those "confined to the interior of the home."[386] In other words, since the court found that the relative impreciseness of the technology did not allow for certain glimpses into the home, *Knotts* and *Karo* dictated that there was no reasonable expectation of privacy in public movements.

At least as support for warrantless access to historical cellular location information, the tracking cases have virtues. In response to critics of the third-party doctrine, they provide a rationale, which comports more easily with reasonable expectations of privacy. Even though the Fourth Amendment "protects people, not places,"[387] one does not have a reasonable expectation of privacy when they occupy public places and spaces because "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[388] For this reason, "in surveying sidewalks, streets and gutters and in roaming the 'open fields' . . . the police would seem to be free to go on fishing expeditions or to go on planned reconnaissances."[389]

The criticism, laid bare in *Maynard*, is that this differs from physical surveillance, because it allows for law enforcement to track all of a person's movements over the course of a long period of time. Ordinary

382. *Id.* at 780.

383. *See* United States v. Graham, 846 F. Supp. 2d 384, 403–04 (D. Md. 2012) (stating that the tracking line of cases also "informs [the] Court's decision," though it primarily relied on the third-party doctrine); *see also* United States v. Salas, No. C RF 11-0354 LJO, 2013 WL 4459858, at *3 (E.D. Cal. Aug. 16, 2013); United States v. Wilson, No. 1:11-CR-53-TCB-ECS-3, 2013 WL 1129199, at *6 (N.D. Ga. Feb. 20, 2013) (discussing the imprecise nature of the tracking data as a "salient fact[]" in the court's decision).

384. *See, e.g.*, *In re* Application of the 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); *Forest*, 355 F.3d at 950–52; United States v. Carpenter, No. 12-20218, 2013 WL 6385838, at *2–3 (E.D. Mich. Dec. 6, 2013); United States v. Moreno-Nevarez, No. 13-CR-0841-BEN, 2013 WL 5631017, at *2 (S.D. Cal. Oct. 2, 2013).

385. In re *Application of the U.S. for an Order to Disclose Records to the Gov't*, 620 F.3d at 319.

386. *Id.* at 312.

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

388. *Id.*

389. 1 LAFAVE, *supra* note 152, § 2.2(a), at 601–02 (quoting Charles E. Moylan, Jr., *The Plain View Doctrine: Unexpected Child of the Great "Search Incident" Geography Battle*, 26 MERCER L. REV. 1047, 1097–98 (1975)).

physical surveillance could not accomplish this due to resource limitations. Given the lack of precision in historical cellular location information,[390] it would clearly be more accurate to simply use physical human surveillance at all times for all targets in an investigation. There are two impracticalities to such an approach. First, the manpower use and cost of physical surveillance is great. As *Kosta* demonstrates,[391] following all the people in a conspiracy, even a relatively small one, is a formidable task.[392] And using historical cellular location information is certainly much more cost-effective than physical surveillance.[393] Meanwhile, the Fourth Amendment implications of this were squarely rejected by *Knotts*, which stated, "Insofar as [the] complaint appears to be simply that scientific devices . . . enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now."[394]

Second, the historical nature of the information sought clearly makes it impossible to use physical surveillance. It does not seem, however, that such a difference has any Fourth Amendment implications. The target of the surveillance wants to claim that law enforcement had its chance to find and track his public location, but did not capitalize and therefore is essentially time-barred under the Fourth Amendment from attempting to gain access to the information now. But this runs contrary to the reasonable expectation of privacy basis of the Court's jurisprudence.[395] One has no more of a reasonable expectation in a record of their public movements than they do in the public movements originally.[396]

390. *See supra* Part II.A.1.

391. *See supra* notes 122–33 and accompanying text.

392. And, of course, law enforcement often focuses on much larger conspiracies. *See, e.g.*, Press Release, U.S. Att'y's Office, Cent. Dist. of Cal., Task Force Investigation Results in Federal and State Charges of MS-13 Gang Members and Associates for Their Roles in a Drug Trafficking Network and Extortion Scheme (Dec. 10, 2013), *available at* http://www.fbi.gov/losangeles/press-releases/2013/task-force-investigation-results-in-federal-and-state-charges-of-ms-13-gang-members-and-associates-for-their-roles-in-a-drug-trafficking-network-and-extortion-scheme (describing the indictment of twenty MS-13 gang members for a methamphetamine distribution conspiracy).

393. *See* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 350 tbl.1 (2014), http://yalelawjournal.org/2014/9/1/bankston-soltani.html (finding the estimated cost of twenty-eight days of covert surveillance from a car to be $184,800 while finding the estimated cost of twenty-eight days of surveillance by using location tracking through AT&T to be $800).

394. United States v. Knotts, 460 U.S. 276, 284 (1983).

395. United States v. Jacobsen, 466 U.S. 109, 122 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.").

396. *Cf.* United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991) (stating where a video surveillance tape was used in a subsequent prosecution that "[v]ideo surveillance does not in itself violate a reasonable expectation of privacy. Videotaping of suspects in public places, such as banks, does not violate the fourth amendment; the police may record what they normally may view with the naked eye").

Where a person is tracked as he traverses public roadways, *Knotts* and *Karo* would seem to be the controlling cases.[397] The trouble, of course, with the tracking justification for historical cellular location information is that it runs headlong into *Karo* and, to a lesser extent, *Kyllo*. Law enforcement will at times use historical cellular location information to corroborate or confirm information they already have about a person's publicly observable location.[398] To the extent that they are trying to discover a person's location during a historical window, however, it is very difficult to determine *ex ante* that the person was not within a place protected by the Fourth Amendment.[399] It can likely be assumed that when a court authorizes collection of historical cellular location information for a time period longer than twenty-four to forty-eight hours, the target will almost certainly have been in a place protected by the Fourth Amendment at some point during that time.

This may not make a difference, however, in the vast majority of cases. As an initial matter, it is unclear that law enforcement frequently has access to[400] or uses[401] historical cellular location information which could indicate a person's location so precisely as to show that they are within a protected area. As we have already established, to the extent that cellular phone companies can locate a customer using GPS capability, this information is typically not retained and therefore is not an issue when examining the standards for historical records.[402] In other words, the majority of historical cellular location information cases will likely not feature data precise enough to raise the specific Fourth Amendment concern addressed in *Karo*.[403]

To the extent that there are tracking cases which do, *Karo* would speak directly to the question of how to treat such information. *Karo*

397. *See supra* notes 178–207 and accompanying text.

398. *See* Sealed Application of the U.S., *supra* note 114 at 2–3 (describing how historical cellular location information will "further the investigation by corroborating the observations of eye witnesses and video cameras operating in the vicinity of the location in which the DEA [Drug Enforcement Administration] is conducting its investigation").

399. The paradigmatic example of a place protected by the Fourth Amendment is the home. Many other places, however, can be protected by the Fourth Amendment. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 301 (1966) (hotel rooms and offices); *see also* O'Connor v. Orteaga, 480 U.S. 709 (1987) (plurality opinion) (places of business not open to the general public).

400. *See Blaze Testimony*, *supra* note 47, at 59 ("A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location will be relatively more or less precise.").

401. For instance, the presentation prepared by FBI Special Agent David M. Magnuson for presentation at the Machado-Erazo trial showed extremely general location information, no more precise than consistent that Machado-Erazo was in a particular neighborhood or town. *See* Cellular Analysis for March 28, 2010 Prepared by SA David M. Magnuson, FBI Headquarters, Cellular Analysis Survey Team, Gov't Exhibit No. 306, United States v. Machado-Erazo, 986 F. Supp. 2d 39 (D.D.C. 2013) ( No. 10-256-08), 2013 WL 5434709, at *10.

402. *See supra* notes 50–56 and accompanying text.

403. *See supra* Part II.A.1.

seems to indicate that the courts should suppress any information, which clearly indicates that the cellular phone (and by extension, the defendant) were in a Fourth Amendment protected area.[404] In *Karo*, the Court agreed with the district court and court of appeals that the information needed to be suppressed, but found that there was enough other tracking and visual surveillance information supporting the warrant to furnish probable cause.[405] Therefore, it is likely that historical cellular location information, which did not locate the targeted person in a protected place, would be admissible.[406]

However, this still leaves courts considering how to treat applications, which almost certainly call for historical cellular location information covering a time period where the target person will be in areas protected by the Fourth Amendment. Therefore, this is potentially a significant problem under *Karo*, since judges should presumably not sign "specific and articulable" court orders, which call for location information, when the Supreme Court has said that it requires probable cause.[407]

Courts have confronted a similar problem in a Fourth Amendment context when considering computer searches.[408] When the police search a computer, they almost inevitably go to the place where the computer is kept, seize the entire computer, and then take it to a digital forensics laboratory to be carefully analyzed—frequently file by file.[409] These searches are subject to search warrants issued in accordance with the Fourth Amendment requirements of probable cause and particularity,[410] but law enforcement will necessarily end up seizing a great deal more information than that which is the subject of the warrant.[411] Like a court order that demands historical cellular location information, some of which will be protected by the Fourth Amendment, so too a search warrant for a computer commands seizure of a huge amount of data, some of

404. United States v. Karo, 468 U.S. 705, 715 (1984) ("For purposes of the [Fourth] Amendment, . . . [an unreasonable search occurs] where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house.").

405. *See supra* notes 202–07 and accompanying text.

406. *See id.*

407. *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (holding that because the court order application calls for information protected by the Fourth Amendment, "the Government's requests for that information under the SCA are denied").

408. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1243–45 (2010) [hereinafter Kerr, *Ex Ante*]; *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532–38 (2005).

409. *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 92–97 (2005).

410. *See* Kerr, *Ex Ante*, *supra* note 408, at 1248.

411. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam) ("We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records.").

which is the subject of the warrant, much of which is not.[412] If overseizing issues do not implicate the Fourth Amendment in the computer context, they should not implicate the Fourth Amendment in the historical cellular location information context either.

Courts have dealt with these warrant requests in a number of ways.[413] While this Note will not consider the actual mechanisms or procedures courts might use to limit the collection of Fourth Amendment protected historical cellular location information, the important takeaway from the computer search cases is that warrants are not denied due to the necessity of overseizing information.[414] On the contrary, courts have recognized that this is an "inherent part of the electronic search process" and have put in place *ex ante* procedures[415] or conducted *ex post* reasonableness analyses[416] to minimize the Fourth Amendment implications of granting such warrants and overseizing. Therefore, any potential *Karo* problem, which might result from overseizing historical cellular location information revealing presence in a Fourth Amendment protected area, can likely be mitigated by suppression, where appropriate, or judicially imposed procedures.[417]

### *C. Mosaic Cases*

Related to the criticisms and concerns of both the third-party doctrine and tracking cases are the so-called "mosaic cases"—i.e., those courts holding that long-term location monitoring can reveal so much about a person that it violates his or her reasonable expectations of pri-

412. *See id.* at 1176 ("Law enforcement today thus has a far more difficult, exacting and sensitive task in pursuing evidence of criminal activities than even in the relatively recent past. The legitimate need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence, is one we've often recognized.").

413. This topic has been the subject of multiple full-length law review pieces and many notes. *See, e.g.*, *supra* notes 408–09.

414. *See, e.g.*, United States v. Banks, 556 F.3d 967, 973 (9th Cir. 2009) ("The prohibition of general searches is not . . . a demand for precise ex ante knowledge of the location and content of evidence . . . The proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation.").

415. *See, e.g.*, *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177, 1179 (Kozinski, C.J., concurring) ("To that end, the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown.").

416. *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (evaluating a computer search *ex post* via a test for reasonableness of the search after stating "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic").

417. A related context where law enforcement regularly overseizes electronic information is when conducting telephone wiretaps under the authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–22 (2012)). This law contains a statutory command that law enforcement "minimize the interception of communications not otherwise subject to interception under this chapter," 18 U.S.C. § 2518(5) (2012); however, the fact that law enforcement will necessarily have to intercept some conversations otherwise protected by the Fourth Amendment does not bar the interception altogether (or lead to the suppression of incriminating conversations). *See* Scott v. United States, 436 U.S. 128 (1978).

vacy and is an intrusion that society is not prepared to recognize as reasonable.[418] These cases often involve extended responses to both the third-party and tracking rationales. *Maynard* was the foundational articulation of the mosaic theory,[419] though other courts and influential judges have endorsed it,[420] and at least two state courts have adopted the mosaic theory as the interpretation of their state constitution.[421]

The decision of the Supreme Judicial Court of Massachusetts concerned the facts introduced earlier in this Note involving the murder trial of Shabazz Augustine.[422] Prior to his trial, Augustine moved to suppress the historical cellular location information collected pursuant to a section 2703(d) order to Sprint.[423] The trial court suppressed the evidence, ruling it violated Article 14 of the Massachusetts Declaration of Rights.[424] The Supreme Judicial Court evaluated the question on interlocutory appeal and agreed,[425] refusing to consider whether the acquisition of historical cellular location information with less than probable cause violated the Fourth Amendment,[426] but squarely holding that "government-compelled production of the defendant's [historical cellular location information] by Sprint constituted a search" under Article 14.[427]

418. *See* Kerr, *Mosaic Theory*, *supra* note 232, at 312–13.

419. *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 581 (E.D.N.Y. 2010) ("I have not previously balked at issuing orders to disclose historical [cellular location information] on a showing of 'specific and articulable facts' pursuant to the SCA in large part because, until now, the federal appellate courts to have addressed the issue have uniformly interpreted [*Knotts*] to hold that location tracking outside the home is analogous to physical surveillance and therefore does not require a warrant. That uniformity no longer exists. The United States Court of Appeals for the District of Columbia Circuit recently reversed the conviction of a defendant on the ground that evidence obtained in violation of his rights under the Fourth Amendment had improperly, and prejudicially, been admitted at trial.") (citations omitted).

420. *See, e.g.*, United States v. Pineda-Moreno, 617 F.3d 1120, 1121–26 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc) (explaining the view of five Ninth Circuit judges that long-term monitoring requires a warrant in the GPS vehicle tracking context, but with discussion of historical cellular location information); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 , 118 (E.D.N.Y. 2011); *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010); *Application of the U.S. for Historical Cell-Site Info.*, 736 F. Supp. 2d at 581.

421. *See* Commonwealth v. Augustine, 4 N.E.3d 846, 850 (Mass. 2014); State v. Earls, 70 A.3d 630 (N.J. 2013).

422. *See supra* notes 134–37 and accompanying text.

423. *Augustine*, 4 N.E.3d at 851.

424. *Id.*

425. *Id.* at 851–52.

426. *Id.* at 858.

427. *Id.* at 866. Article 14 of the Massachusetts Declaration of Rights states: "Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws." MASS. CONST. Pt. I, art. XIV (West 2014). The language of Article 14 was enacted in 1780 prior to the United States Constitution and "closely anticipate[s]" the language of the Fourth Amendment. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 763 n.10 (1994).

The court first examined the nature of cellular phone use and concluded that cellular phones are "indispensable part[s] of modern [American] life"[428] that "physically accompany their users everywhere—almost permanent attachments to their bodies."[429] The court then found that historical cellular location information tracked a person's location and therefore implicated substantial privacy concerns, likely even more than the GPS tracker at issue in *Jones*.[430]

The court distinguished between the cellular phone technology at issue and the third-party doctrine cases like *Smith* and *Miller*.[431] The court found that in *Smith*, the telephone numbers at issue were only that which the person "knowingly provided to the telephone company when he took the affirmative step of dialing the calls"; therefore "[t]he information conveyed . . . was central to the subscriber's primary purpose for owning and using the . . . telephone: to communicate with others."[432] The court continued that in the historical cellular location information context, no person "voluntarily conveys [historical cellular location information] to his or her cellular service provider in the sense that he or she first identifies a discrete item of information . . . like a telephone number . . . and then transmits it to the provider."[433] Instead, the court conceived of historical cellular location information as "purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects to a cell site."[434] Therefore it bears "no connection at all to the reason people use cellular telephones."[435] The court then quoted the New Jersey Supreme Court in *State v. Earls*: "People buy [cellular telephones] to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a [cellular telephone] to share detailed information about their whereabouts with the police."[436] With this, the Massachusetts Supreme Judicial Court found the third-party doctrine inapplicable in the context of historical cellular location information.[437]

From there, it was a *fait accompli* that historical cellular location information would be subject to the warrant requirement under the Fourth Amendment. The court raised successive concerns about the tracking of a person in Fourth Amendment protected spaces,[438] the historical nature

428. *Augustine*, 4 N.E. 3d at 859 (quoting State v. Earls, 70 A.3d 630, 643 (N.J. 2013)).
429. *Id.*
430. *Id.* at 860–61.
431. *Id.* at 862–63. The court acknowledged earlier in the opinion that traditionally it had applied the third-party doctrine in full to Article 14, though it had left the door open to a more limited interpretation in the future. *Id.* at 858 (citing Commonwealth v. Cote, 556 N.E.2d 45 (Mass. 1990)).
432. *Id.* at 862.
433. *Id.*
434. *Id.*
435. *Id.*
436. *Id.* at 862–63 (alterations in original) (quoting State v. Earls, 70 A.3d 630, 643 (N.J. 2013)).
437. *Id.* at 863.
438. *Id.* at 864 ("[W]e cannot ignore the probability that, as CSLI becomes more precise, cellular telephone users will be tracked in constitutionally protected areas.").

of information obtained,[439] and, finally, the amount of time for which Augustine was tracked.[440] Without resting on one rationale for finding a reasonable expectation of privacy, the Supreme Judicial Court of Massachusetts concluded that such a reasonable expectation existed and therefore "the government-compelled production of the defendant's [historical cellular location information] by Sprint constituted a search in the constitutional sense to which the warrant requirement of art. 14 applied."[441]

Just a few months earlier, the New Jersey Supreme Court found similarly.[442] Though the court acknowledged that current U.S. Supreme Court jurisprudence would likely not require a warrant, the Court fully embraced the mosaic theory in deciding that location data requires a warrant under the New Jersey Constitution.[443] In doing so, the New Jersey Supreme Court reaffirmed the narrow nature of the third-party doctrine in New Jersey.[444] The court found that "cell-phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[445] People therefore have a "reasonabl[e] expect[ation] that their personal information will remain private."[446] Finding therefore that cellular phones provide "an intimate picture of one's daily life" and are "an indispensable part of modern life,"[447] the court found that a warrant would be required for historical cellular location information under the New Jersey Constitution.[448]

Shortly before *Riley*, the U.S. Court of the Appeals for the Eleventh Circuit issued its opinion in *United States v. Davis*, a ruling that relied largely on something like the mosaic theory in holding that obtaining historical cellular location information required a warrant.[449] Quartavius

439. *Id.* at 865 ("[W]hen the government obtains historical CSLI from a cellular service provider, the government is able to track and reconstruct a person's past movements, a category of information that *never* would be available through the use of traditional law enforcement tools of investigation.").

440. *Id.* ("[I]t is likely that the duration of the period for which [historical cellular location information] is sought will be a relevant consideration in the reasonable expectation of privacy calculus—that there is some period of time for which the Commonwealth may obtain a person's historical CSLI by meeting the standard for a [Section] 2703(d) order alone, because the duration is too brief to implicate the person's reasonable privacy interest. But there is no need to consider at this juncture what the boundaries of such a time period might be in this case because, for all the reasons previously rehearsed concerning the extent and character of cellular telephone use, the two weeks covered by the [Section] 2703(d) order at issue exceeds it . . . .").

441. *Id.* at 866.

442. State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

443. *Id.* at 644. The New Jersey Constitution, the court says, is "nearly identical," though the New Jersey Supreme Court does not interpret its own constitution identically to the U.S. Constitution. *Id.* at 641.

444. *Id.* at 641.

445. *Id.*

446. *Id.*

447. *Id.* at 642–43.

448. *Id.* at 644.

449. United States v. Davis, 754 F.3d 1205, 1210–17, *vacated and reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014). Interestingly, the panel decision in *Davis* was written by Judge Sentelle of

Davis had been convicted on sixteen counts connected to a series of armed robberies of stores, restaurants, and gas stations and sentenced to 1941 months in federal prison.[450] As we have seen is often the case, testimony regarding the location of Davis' cellular phone buttressed an already strong case. Davis' coconspirators testified against him, as did eyewitnesses to the robberies.[451] The government showed surveillance tapes purporting to show Davis committing the robberies and presented DNA evidence tying Davis to the getaway car.[452]

The panel in *Davis* began by weighing the import of the Fifth Circuit's decision in *In re Application of the United States for Historical Cell Site Data* before concluding, "[w]e will not review at this point the reasoning . . . given that the context of the cases is different."[453] This was a reference to the *ex parte* nature of the proceedings at issue in the Fifth Circuit's case; however, this is a very curious choice by the Eleventh Circuit's panel. The question presented by the cases is the exact same, but with this terse dismissal of the relevance of the Fifth Circuit's decision, the court in *Davis* ceased to consider it in its reasoning.

The Eleventh Circuit considered and quoted from *Jones* at length in its decision, but then took the reasoning of *Jones* even further, finding that, in this case, because of the nature of historical cellular location information, "[s]uch a mosaic theory is not necessary to establish the invasion of privacy in the case of cell site location data."[454] The panel continued:

> [O]ne may assume that [certain] visit[s, such as those to a doctor or priest, are] private if . . . not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts. Therefore . . . even one point of cell point location data can be within a reasonable expectation of privacy. . . . [I]t is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.[455]

As private data, therefore, the panel concluded that government acquisition of this data was a search and required a warrant.[456] Though for a short time, this created a circuit split with the Fifth Circuit on the prima-

the U.S. Court of Appeals for the D.C. Circuit when he was sitting by designation on the 11th Circuit. *Id.* at 1208.

450. *Id.* at 1209–10.
451. *Id.* at 1209.
452. *Id.*
453. *Id.* at 1211–12.
454. *Id.* at 1215.
455. *Id.* at 1216.
456. *Id.* at 1217.

ry topic of this Note, the Eleventh Circuit vacated this panel decision in order to rehear the case en banc in September 2014.[457]

The mosaic theory responds to the shortcomings of the third-party doctrine and location tracking cases.[458] It responds to the rapid technological changes since those cases (which are now almost all thirty years old) and a world in which we increasingly rely on third parties to act as custodians of large amounts of personal information.[459] Most importantly, in keeping with *Katz*, it may actually fulfill society's "reasonable expectation of privacy."[460] A cellular phone is so necessary in today's society that few people would think that by acquiring one, they present law enforcement with the opportunity to gain access to a vast record of their personal habits.[461] As the use of this data grows,[462] it will only become more powerful and thus the expectations of privacy will rise.

Professor Kerr, however, has provided a pointed criticism of the mosaic theory on several grounds.[463] First, Kerr argues that the "mosaic theory" represents a rejection of the sequential approach to adjudicating Fourth Amendment questions.[464] Under the sequential approach, each separate investigative step is evaluated independently to gauge if it would violate the Fourth Amendment.[465] This standard is easily administered and bright-line rules work best for law enforcement because in the midst of stressful and high-stakes investigations, clear guidance from the courts and legislature about what is legally required reduces oversteps and mistakes.[466] It is also simply a traditional and well-honored method of Fourth Amendment analysis, recognizing the reality that different moti-

457. United States v. Davis, No. 12-12928, 2014 WL 4358411, at *1 (11th Cir. Sept. 4, 2014).

458. For criticisms of the third-party doctrine and location tracking, many of which were articulated in *Augustine* and *Maynard* as the drivers of the mosaic theory, see *supra* Parts III.A–B.

459. *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1315–18 (2012).

460. *Government and Corporate Surveillance Draw Wide Concern*, WASH. POST, Dec. 22, 2013, http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/12/21/National-Politics/Polling/release_282.xml (detailing that sixty-nine percent of those polled indicated they were "[v]ery concerned" or "[s]omewhat concerned" about "the government . . . collecting digital information from your . . . phone").

461. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002) ("The complete benefits of the Information Age do not simply come to us. . . . [W]e must establish relationships with a panoply of companies.").

462. *See* Haoyi Xiong et al., *Predicting Mobile Phone User Locations by Exploiting Collective Behavorial Patterns*, 9TH INT'L CONF. ON UBIQUITOUS INTELLIGENCE & COMPUTING & 9TH INT'L CONF. ON AUTONOMIC & TRUSTED COMPUTING 164, 166–70 (2012), *available at* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6331976 (describing methods to determine future associations and locations by analyzing past cellular location information).

463. *See* Kerr, *Mosaic Theory*, *supra* note 232, at 311.

464. *See id.* at 315–20.

465. *Id.* at 316. For instance, when confronted with twenty-eight consecutive days of historical cellular location information tracking, a court would ask if at any time (on any one day) did that investigative activity constitute a "search." *Id.* If not, the court would find that no search had occurred, instead of presumably considering the information in the aggregate under the mosaic theory. *Id.*

466. *See* Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 4 (2013).

vations and circumstances attend to different events for Fourth Amendment purposes and thus those events must be analyzed separately.[467]

Second, the mosaic theory's new approaches to the time and seriousness of investigations will also cause issues. As Justice Scalia pointed out in response to Justice Alito in *Jones*, this introduces a host of "vexing problems" that will burden law enforcement.[468] How long can a suspect be investigated before the mosaic theory is implicated? Does the type of offense matter? "What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?"[469] And, as Kerr points out, how do we group different investigative techniques together? "If seven days of continuous GPS monitoring creates a mosaic search, how should courts treat, say, six days of combined monitoring and one day of visual monitoring? Does that count as ten days' worth of monitoring, or only six?"[470] These questions, of course, are not insurmountable. Judges and law enforcement routinely evaluate Fourth Amendment concepts, such as the existence of probable cause, based upon the "totality of the circumstances" instead of a sequential or uniform standard.[471] They underline, however, what a sharp departure this jurisprudence would be from the present paradigm.

A much more basic problem lies in the mosaic theory, especially as conceived of by the Supreme Judicial Court of Massachusetts. The court there continued to rely on several of the fallacies exposed above: that historical location records have different Fourth Amendment implications than present records,[472] that historical cellular location information revealing presence in a protected area should eliminate the possibility of gaining access to nonprotected information,[473] and, finally, that cellular phone users do not "voluntarily"[474] convey their location to their cellular phone company; that location information is not "connect[ed]"[475] to their reason for using the cellular phone, and that "no one buys a [cellular telephone] to share detailed information about their whereabouts with the police."[476] These three main arguments have been refuted in the prior discussion of the third-party doctrine and tracking cases; we pause briefly, however, to consider how strained the last argument is. Far from be-

467. *See, e.g.*, United States v. Wright, 739 F.3d 1160, 1172 (8th Cir. 2014) (Riley, C.J., concurring) ("Officers entered Wright's home without a warrant not once, but twice. The first time, as the district court concluded, exigent circumstances justified the entry. . . . The second time police officers entered, there was no justification for the warrantless search.").

468. United States v. Jones, 132 S. Ct. 945, 953–54 (2012) (internal quotation marks omitted).

469. *Id.* at 954.

470. *See* Kerr, *Mosaic Theory*, *supra* note 232, at 336.

471. *See* Illinois v. Gates, 462 U.S. 213, 232 (1983) ("[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.").

472. *See supra* Part II.B.

473. *See supra* Part III.B.

474. Commonwealth v. Augustine, 4 N.E.3d 846, 862 (Mass. 2014).

475. *Id.*

476. *Id.* at 863 (quoting State v. Earls, 70 A.3d 630, 643 (N.J. 2013)).

ing a byproduct, the ability of your cellular phone company to locate you all over the country, indeed, all over the world—in your home, but also in public spaces and other people's homes—*is* the reason people acquire cellular phones. The convenience and necessity of a cellular phone is entirely connected to the fact that your cellular phone company will deliver communications and information to you no matter where you are, as long as you have signal strength—meaning, of course, that you are close enough to a cellular tower to communicate with it. As for the final statement, that people do not purchase cellular phones to share their location with the police, it is difficult to see what would not be protected by the Fourth Amendment, if such a standard was in place. Criminals almost never seek to share incriminating information with the police, but when they operate in public or draw upon third-party resources, they are not shielded from the law.[477] As the Supreme Court has counseled, "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities."[478] Lastly, the proposition that people do not realize they share this crucial and inherent information with their cellular phone company is, at the least, very debatable.[479]

## IV. RECOMMENDATIONS

What follows is a series of modest recommendations. While the Fourth Amendment implications of technology are a serious and pressing concern, it does not follow that we should rush into an alteration of the dominant Fourth Amendment paradigm through judicial power. Instead, as the above analysis has demonstrated, the Fourth Amendment issues surrounding historical cellular location information do not call for an overhaul of the Fourth Amendment. Rather, they call for a series of first steps, which can be evaluated by legislatures and the public as they gauge the correct balance between privacy and security.

477. The court in *Augustine* also endorsed its past applications of the third-party doctrine as still good law; however, it is hard to see how these precedents could survive under the aforementioned standard. *See id.* Certainly no one opens a bank account in order to share their financial information with the police, nor does one dial a phone number in order to share their assocations with the police.

478. United States v. Jacobsen, 466 U.S. 109, 122 (1984).

479. JAN LAUREN BOYLES ET AL., PEW RESEARCH CTR., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES 2 (2012), http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf (finding that in 2012, nineteen percent of cellular phone users had disabled location tracking on their phone in response to concerns about the uses of that information by third parties).

### *A. Create a Statutory Suppression Remedy in the Stored Communications Act*

As discussed above, the SCA, as presently constituted, contains no suppression remedy.[480] As such, if historical cellular location information is collected pursuant to a flawed, conclusory, or even patently false court order, there is no mechanism to keep this evidence out of court.[481] The traditional rationales underlying the exclusion of evidence obtained contrary to statute or the Constitution, therefore, do not apply in this context.[482] As the Supreme Court has recognized, "Nothing can destroy a government more quickly than its failure to observe its own laws."[483] There is a second problem, however. Namely, the judiciary will seek to fill the obvious void by constitutionalizing this area of the law, declaring historical cellular location information subject to the Fourth Amendment, and applying the exclusionary rule against this conduct.[484] To avoid these issues, Congress should take action and provide a suppression remedy in the SCA.

### *B. Rely on Legislatures—Federal and State—to Remedy Excesses in the Acquisition of Historical Cellular Location Information*

William J. Stuntz wrote compellingly about the failures of the over-constitutionalization of criminal procedure.[485] This process stemmed from a belief that "elected legislators would never adequately protect the interests of criminal suspects and defendants."[486] Stuntz argued, however, that this was false, writing, "Legislators respond to powerful interest groups. Contrary to the conventional wisdom, criminal suspects *are* a powerful interest group. The police stop 23 million motorists per year. . . . [N]o politician can afford to ignore the interests of that many constituents."[487] Now consider data that indicates ninety percent of adults in the United States use a cellular phone.[488]

Professor Kerr has demonstrated that in the context of new technologies—in his case study, wiretapping—Congress, not the courts, has

480. Kerr, *User's Guide*, *supra* note 95, at 1241.

481. *Id.*; *see* United States v. Guerrero, 768 F.3d 351, 357–59 (5th Cir. 2014) (acknowledging no suppression remedy under the SCA where historical cellular location information was obtained in clear violation of the SCA).

482. *See* Mapp v. Ohio, 367 U.S. 643, 656–59 (1961).

483. *Id.* at 659.

484. William J. Stuntz has written about this process. *See* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780, 791–92 (2006) ("When the Supreme Court constitutionalized criminal procedure in the 1960s the conventional wisdom, evidently shared by the Justices, held that elected legislators would never adequately protect the interests of criminal suspects and defendants. . . . Today, the Justices' political prophecy looks either wrong or self-fulfilling.").

485. *Id.*

486. *Id.*

487. *See id.* at 795 (footnotes omitted) (emphasis in the original).

488. *Mobile Technology Fact Sheet*, PEW RES. INTERNET PROJECT, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Oct 24, 2014).

taken the lead in protecting privacy.[489] Indeed, in the realm of historical cellular location information, legislatures have already begun to do so. Congress has conducted inquiries and investigations,[490] held hearings,[491] and proposed legislation[492] to require a search warrant for "information . . . concerning the location of a wireless communication device . . . that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person."[493]

Furthermore, state legislatures have become active in this area, as well. In May 2013, Montana became the first state[494] to enact legislation that required law enforcement to obtain a warrant in order to access, in almost all instances, location information, defined broadly as "information concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device."[495] If obtained without a warrant, violators are exposed to a civil penalty, as well as a bar against using the evidence in any "criminal, civil, or administrative proceeding," *or* in the affidavit for a search warrant.[496]

The California legislature passed a similar bill in 2012,[497] while Maine has since followed suit and enacted its own law prohibiting the acquisition of cellular location information.[498] At least twelve other states have considered similar measures,[499] a number which will surely increase as public and legislative knowledge of the issue grows.

It is axiomatic in our federalist system that states serve as "laboratories of democracy," experimenting with more or less protection for certain actions.[500] In this spirit, Montana and Maine will serve as bellwethers.

489. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 839–40 (2004); *see also* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in judgment) ("Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing [wiretapping]. Instead, Congress promptly enacted a comprehensive statute, and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law." (citation omitted)).

490. *See* Markey Press Release, *supra* note 53.

491. *See Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1 (2013).

492. To Amend Title 18, United States Code, to Specify the Circumstances in Which a Person May Acquire Geolocation Information and for Other Purposes, H.R. 1312, 113th Cong. (2013).

493. *Id.* §§ 2601(3), 2602(h)(2).

494. Somini Sengupta, *With Montana's Lead, States May Demand Warrants for Cellphone Data*, N.Y. TIMES BITS BLOG (July 2, 2013, 5:24 PM), http://bits.blogs.nytimes.com/2013/07/02/with-montanas-lead-states-may-demand-warrants-for-cellphone-data/?_php=true&_type=blogs&_r=0.

495. An Act Providing that a Government Entity Must Obtain a Search Warrant Prior to Obtaining Location Information of an Electronic Device; and Providing Exception, Definitions, and a Civil Penalty, 2013 Mont. Laws. ch. 394 (codified at MONT. CODE. ANN. § 46-5-110 (West 2014)).

496. *Id.* § 46-5-110(1)(c)–(d).

497. Sengupta, *supra* note 494.

498. 2013 Me. Laws. ch. 409 (codified at ME. REV. STAT. ANN. tit. 16, §§ 641–646-B (2013)).

499. Sengupta, *supra* note 494.

500. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("To stay experimentation in things social and economic is a grave responsibility. Denial of the right to ex-

Maybe law enforcement will be greatly hindered by these requirements. Maybe, however, law enforcement will see only negligible increases in investigative burdens as they already requested these records with "specific and articulable facts" approaching probable cause.[501] Legislatures can respond nimbly and perceptively to these concerns—conducting hearings and investigations and debating through proposed legislation. As Justice Alito recognized in his concurrence in *Jones*, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[502]

### *C. Law Enforcement Should Consider Imposing its Own Standards*

Some law enforcement agencies and prosecutors' offices have begun unilaterally requiring a warrant before their investigators access historical cellular location information.[503] Police frequently use historical cellular location information to buttress already strong criminal cases.[504] In these circumstances, it is highly likely that police would be able to obtain a warrant for this information. Therefore, most high-profile investigations may not be affected by the warrant requirement at all.

People abide by and respect laws that they believe to be legitimate.[505] Tom Tyler, a noted sociologist, has found that "[p]rocedural justice is the key normative judgment influencing . . . legitimacy."[506] In evaluating procedural justice, in other words, whether fair procedures were followed in making a decision which affects people, Tyler found that several factors are very important. Among them is "a belief on the part of those involved that they had an opportunity to take part in the decision-making process. This includes having an opportunity to present their arguments, be[] listened to, and hav[e] their views considered by the authorities."[507] Similarly important is the "neutrality of the decision-making process" and "inferences about the motives of the authorities."[508]

periment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

501. *See supra* notes 98–101 and accompanying text.

502. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in judgment) (citation omitted).

503. *See, e.g.*, Letter from Karen H. Steed, Assistant Records Custodian, Lexington Fayette Urban Cnty. Div. of Police, to William E. Sharp, Staff Att'y, ACLU of Ky. (Aug. 16, 2011) *available at* https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_lexingtonpd_lexingtonky.pdf ("In regard to the acquisition of cell phone location records, data, and/or information, [the policy of the Lexington Division of Police is that] such items can be obtained only with a search warrant.").

504. *See supra* Part II.D.

505. TOM R. TYLER, WHY PEOPLE OBEY THE LAW 170 (1990).

506. *Id.* at 162.

507. *Id.* at 163.

508. *Id.* at 163–64.

Law enforcement can take lessons from these findings and apply them to historical cellular location information. Agencies, which require a warrant for this information, could potentially play to all three of these aforementioned concerns. The warrant procedure is found in the Constitution,[509] considered the people's document.[510] Though warrants are approved in *ex parte* proceedings, suppression hearings and other proceedings to address the appropriateness of a warrant allow people the opportunity to be heard and present arguments.[511] Furthermore, concerns about a neutral decision maker and the motives of authorities would be well addressed by the warrant requirement—particularly one that is self-imposed—as it "provides the detached scrutiny of a neutral magistrate, which is a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer engaged in the often competitive enterprise of ferreting out crime."[512]

## V. CONCLUSION

The government's ability to compel disclosure of historical cellular location information from cellular phone companies is just one front in the struggle to interpret Fourth Amendment protections in light of rapidly evolving technology. Multiple strands of Fourth Amendment jurisprudence, including the third-party doctrine and tracking cases, are all implicated in this analysis. As this Note has shown, however, the protections of the Fourth Amendment do not cover this location information properly. In this case, it would likely behoove Congress, state legislatures, and law enforcement to work towards a greater protection for this information. Based on what information is publicly available, it seems likely that law enforcement loses little by seeking a warrant based on probable cause in many cases. In return, they would retain legitimacy and public trust—valuable commodities in a country increasingly concerned about the reach of government monitoring into our private lives.

509. U.S. CONST. amend. IV.

510. *See* McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 403 (1819) ("From these Conventions the constitution derives its whole authority. The government proceeds directly from the people; is 'ordained and established' in the name of the people . . . ."); *see also* Hawke v. Smith, 253 U.S. 221, 226 (1920) ("The Constitution of the United States was ordained by the people, and, when duly ratified, it became the Constitution of the people of the United States.").

511. *See* Franks v. Delaware, 438 U.S. 154, 155–56 (1978).

512. United States v. Leon, 468 U.S. 897, 913–14 (1984) (internal quotation marks omitted).