Hofstra Law Review

Volume 43 | Issue 4 Article 8

1-1-2015

Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps

Amanda Regan

NOTE

DUMPING THE PROBABLE CAUSE REQUIREMENT: WHY THE SUPREME COURT SHOULD DECIDE PROBABLE CAUSE IS NOT NECESSARY FOR CELL TOWER DUMPS

I. INTRODUCTION

With technology changing and improving as quickly as ever, it stands to reason that the law is often behind the times, and regularly needs to catch up.[1] This is precisely where the law currently stands regarding cell phones.[2] It seems as though cell phone technology improves on a regular basis.[3] These changes result in laws that are outdated and a need for increased scrutiny by the courts.[4] Estimates suggest that in 2013, there were approximately 335.65 million wireless subscriber connections.[5] Additionally, there were nearly 304,360 cell towers in the United States.[6] In 2012, Verizon Wireless received an estimated 270,000 law enforcement requests for information about

1. *See* Jeffrey S. Sutton, *Courts, Rights, and New Technology: Judging in an Ever-Changing World*, 8 N.Y.U. J. L. & LIBERTY 261, 262-63 (2014); *see also* Caitlin Rice, *Police In My Pocket: The Need For Fourth Amendment Protection For Cellular Telephone Tracking*, CHAMPION, Nov.–Dec. 2014, at 36, 36, 40 (discussing how the Supreme Court has not confronted the issue of whether nonphysical surveillance, such as cellular GPS tracking, constitutes a search).

2. *See Privacy*, ELECTRIC FRONTIER FOUND., https://www.eff.org/issues/privacy (last visited Sept. 2, 2015).

3. *See* James Kendrick, *Mobile Technology: The Amazing Impact on Our Lives*, ZDNET (Apr. 30, 2013, 10:55 AM), http://www.zdnet.com/mobile-technology-the-amazing-impact-on-our-lives-7000014679.

4. *See* Sutton, *supra* note 1, at 263-64.

5. *Your Wireless Life: Annual Wireless Industry Survey*, CTIA WIRELESS ASS'N, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited Sept. 2, 2015) (explaining that wireless subscriber connections include the number of active devices, such as smartphones, feature phones, and tablets, but because many users have more than one device, this number is not reflective of the number of individual subscribers).

6. *Id.*

customers' cell phone usage.[7] Similarly, AT&T received 301,816 federal, state, and local criminal and civil investigation demands for cell phone information.[8]

One of the most pressing cell phone-related issues involves a practice known as "cell tower dumps."[9] Cell tower dumps have been described as "a limited dragnet."[10] When law enforcement requests cell-site location data, or a cell tower dump, they are requesting the information on all calls transmitted through a cell tower at a given time, on a given date, near a specific location.[11] Cell tower dumps are considered to be a subset of historical cell-site information.[12] This differs from the more typical law enforcement requests for cell-site location data, which involves the call information for a particular cell phone number provided by law enforcement.[13] When government officials

7. Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Edward Markey, Senator of Mass. 1 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf (dividing those requests into 135,000 for "subscriber information or historical call detail records," and 30,000 for "location information and 'cell tower dumps'"). Historical call detail information and subscriber information is information that is customarily divulged on a customer's bill. *Id.*

8. *AT&T Transparency Report*, AT&T INC. 3-4, http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_Jan%202014.pdf (last visited Sept. 2, 2015) (dividing the requests AT&T fulfilled into 24,229 historical cell-site location information demands, 12,576 real-time cell-site location information demands, and 1,034 cell tower searches). Historical cell-site location information allows law enforcement to get information about a person's past communications and locations. Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1884 (2011). Real-time cell-site location provides law enforcement with a person's approximate location at that exact moment. *Id.*

9. *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 3-6 (2013) (describing how cell tower dumps work); *see also* Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of 'Tower Dumps,'* WASH. POST, Dec. 9, 2013, at A1.

10. Nate Anderson, *How "Cell Tower Dumps" Caught the High County Bandits—and Why It Matters*, ARS TECHNICA (Aug. 29, 2013, 8:00 AM), http://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters.

11. Nakashima, *supra* note 9; *see also* John Kelly, *Cellphone Date Spying: It's Not Just the NSA*, USA TODAY (June 13, 2014, 2:40 PM), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809. The practice of using cell tower dumps as an investigatory technique has become so common that:

> About one in four law-enforcement agencies have used a tactic known as a "tower dump," which gives police data about the identity, activity, and location of any phone that connects to the targeted cellphone towers over a set span of time, usually an hour or two. A typical dump covers multiple towers, and wireless providers, and can net information from thousand of phones.

See Kelly, *supra.*

12. *In re* United States, 42 F. Supp. 3d 511, at 512-13 (S.D.N.Y. 2014) (explaining the difference between typical requests for historical cell-site information and cell tower dumps).

13. Peter A. Crusco, *Cell Tower Dumps and the Fourth Amendment*, 251 N.Y.L.J. 5, 5 (2014).

request a cell site info, they obtain a list of calls made to and from the given telephone number, along with the location of the cell towers from which the calls originated and terminated.[14] Generally, law enforcement requests cell-site information for periods of thirty minutes or less.[15]

In contrast, when law enforcement requests a cell tower dump, they generally do not know a targeted suspect's cell phone number.[16] Therefore, in order to identify a suspect, law enforcement must go through the cell service provider records and determine all cell phone numbers that are in the vicinity of the cell tower on the date and time in question.[17] This data may generate additional evidence that could help them find a suspect and establish probable cause.[18] The records obtained via cell tower dumps commonly let law enforcement know the neighborhood the phone was located in when the call was placed and when the call ended.[19] Thus, cell tower dumps can be an extremely useful investigatory tool for crimes such as home invasions, robberies, or sexual assaults.[20]

The forms of cell-site location data law enforcement can request are real-time[21] and historical.[22] The distinctions between historical and real-

14. *Id.*

15. Brief for ACLU at 6, *In re* United States, 42 F. Supp. 3d 511 (S.D.N.Y. 2014) (No. M-50), *available at* https://www.aclu.org/sites/default/files/assets/5.20.2014_ aclu_tower_dump_brief_ to_m.j._francis.pdf (explaining when the time requested exceeds thirty minutes, service providers might request that law enforcement narrows the scope).

16. Crusco, *supra* note 13, at 5.

17. Owsley, *supra* note 9, at 6.

18. Crusco, *supra* note 13, at 5 (discussing two cases where law enforcement used cell tower dumps to establish probable cause); *see also* Jeff Stone, *NYPD Investigating Brooklyn Bridge White Flags Mystery with 'Invasive' Cell Tower Surveillance, Worrying Privacy Advocates*, INT'L BUS. TIMES (July 29, 2014, 3:32 PM), http://www.ibtimes.com/nypd-investigating-brooklyn-bridge-white-flags-mystery-invasive-cell-tower-surveillance-1642520 (discussing that cell tower dumps proved to be particularly helpful in solving the murder of Imette St. Guillen when prosecutors used data from a nearby cell tower to prove Daryl Littlejohn traveled from his home to the place where the body was found).

19. Orin Kerr, *The Eleventh Circuit's Novel Approach to the Fourth Amendment in the Davis Case*, VOLOKH CONSPIRACY (June 19, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/19/the-eleventh-circuits-novel-approach-to-the-fourth-amendment-in-the-davis-case.

20. Owsley, *supra* note 9, at 6 (explaining how cell tower dumps are useful in these sorts of "serial crimes" because law enforcement can "cross-reference for numbers that come up in all locations"). Recently, the New York City Police Department used cell tower dumps to determine who placed white flags on the Brooklyn Bridge. Stone, *supra* note 18. In Colorado, police caught the "High Country Bandits" by using cell tower dumps to help solve a series of sixteen robberies. Anderson, *supra* note 10.

21. Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1748 (2009). Real-time cell-site location information allows law enforcement to obtain information about a person's communications and locations "as it happens in real time." *Id.* Real-time cell-site information is a branch of prospective cell-site information, referring to cell-site information "that is

time cell-site location data are significant because the courts tend to treat the expectation of privacy and level of protection needed differently depending on the type of information being requested.[23] Since cell tower dumps are a subset of historical cell-site location data, this Note will focus more closely on the treatment of historical cell-site information by the law and the courts.[24] Historical cell-site information allows law enforcement to get information about a person's past communications and locations.[25] Often, historical cell-site location data "involves using historical call detail records [] to identify the location and pattern of movements over time of relevant cell phones 1) within mapped radio frequency [] areas, 2) relative to geographically-fixed cell towers, and 3) at fixed points in time."[26] Historical call detail records provide precise information regarding date, time, and location of a cell phone.[27] Additionally, historical call detail records provide all incoming and outgoing telephone numbers that connect with the cell tower, including both voice calls and text messages.[28] These records provide how long these connections lasted, as well as the cell towers that the cell phone was connected to at the beginning and end of these connections.[29]

---

generated after the government has received court permission to acquire it." *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 402 F. Supp. 2d 597, 599 (D. Md. 2005). Further, real-time cell-site location information "would reveal the physical location of the person in possession of the cell phone whenever the phone was on." *Id.* at 598. Some courts have determined that real-time cell-site location information is akin to cell phone tracking and, therefore, requires a showing of probable cause to obtain a warrant. *Id.* at 604-05. Generally, real-time cell-site location information is considered to be "a more invasive search." Rice, *supra* note 1, at 37.

22. Harkins, *supra* note 8, at 1884 (explaining that the distinction between real-time and historical cell-site location information becomes important in light of the privacy interest of the person targeted).

23. Rice, *supra* note 1, at 37.

24. *In re* United States, 42 F. Supp. 3d 511, 512-13 (S.D.N.Y. 2014); *see infra* Part III.B.

25. Chamberlain, *supra* note 21, at 1748.

26. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. ATT'YS' BULL., Nov. 2011, at 16, 16 (2011).

27. *Id.* at 26.

28. *Id.* Law enforcement requests historical cell data records because:

> Cell tower and cell sector information for a particular cell phone is recorded in [historical cell data records] CDRs at the time (1) a voice call is initially connected, (2) a voice call is terminated, (3) a connection is made with the voice mail message service to leave or retrieve a voice message, (4) a text message is sent, and (5) a text message is delivered, which may be different than the time that the cell phone user reads the text message.

Id.

29. *Id.*

The practice of cell tower dumps raises the question of whether they violate a person's reasonable expectation of privacy and are, therefore, a search under the Fourth Amendment.[30] The Supreme Court has established a two-prong test to determine whether something is a search under the Fourth Amendment: (1) does the person have an actual expectation of privacy; and (2) is society prepared to recognize that expectation of privacy as reasonable.[31]

The current court cases dealing with cell tower dumps focus on the standard necessary to obtain cell tower dumps, but these court-imposed standards are inconsistent and unclear.[32] Some courts have determined that law enforcement is required to show "specific and articulable facts"[33] to conduct a cell tower dump, whereas other courts have determined that cell tower dumps can only be obtained upon a showing of probable cause.[34] Adding to this confusion, many wireless service providers require standards other than those required by statutes or the courts.[35] To eliminate this confusion, the Supreme Court should establish a bright line rule.[36] The rule needs to provide law enforcement with a clear guideline to follow for requesting cell tower dumps.[37] A specific

30. *See* Crusco, *supra* note 13, at 5.

31. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

32. *See* Nakashima, *supra* note 9, at A9.

33. *In re* U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010); *see also In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

34. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014), *aff'd* 785 F.3d 498 (11th Cir. 2015) (en banc); *see also In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 605-06.

35. *See* Letter from William B. Petersen to Edward Markey, *supra* note 7; *AT&T Transparency Report*, *supra* note 8; *Verizon's Transparency Report for the Second Half of 2014*, VERIZON WIRELESS, http://transparency.verizon.com/us-report?/us-data (last visited Sept. 2, 2015) [hereinafter *Verizon's Transparency Report*]. Both Verizon and AT&T require law enforcement to provide a warrant or a court order when requesting location information. *AT&T Transparency Report*, *supra* note 8; *Verizon's Transparency Report*, *supra*. Verizon only requires that a judge sign the warrant or court order. Letter from William B. Petersen to Edward Markey, *supra* note 7. However, AT&T will only release location information upon a warrant or court order based on probable cause. *AT&T Transparency Report*, *supra* note 8. When law enforcement can show an emergency exists, Verizon and AT&T will provide cell tower information without a warrant or court order. *See* Letter from William B. Petersen to Edward Markey, *supra* note 7; *AT&T Transparency Report*, *supra* note 8. Verizon requires that law enforcement certify in writing that "pursuant to federal law there was an emergency involving the danger of death or serious physical injury that required disclosure without delay." Letter from William B. Petersen to Edward Markey, *supra* note 7. AT&T also requires law enforcement certification that they are investigating a case involving the risk of death or serious injury. *AT&T Transparency Report*, *supra* note 8. Further, AT&T specifies emergencies as being "kidnappings, missing person cases, attempted suicides, and other emergencies." *Id.*

36. *See infra* Part IV.A.

37. *See infra* Part IV.A.

and articulable facts standard should be required in order for law enforcement to obtain cell tower dumps.[38]

This Note will begin by examining the current state of the law concerning cell tower dumps and the Fourth Amendment by analyzing the legislative initiatives and judicial interpretations pertaining to cell tower dumps.[39] Part II will examine current legislation and proposed legislation on the subject of cell tower dumps.[40] It will then examine judicial jurisprudence regarding the Fourth Amendment and technology in recent history.[41] Part III will explore the problems with determining the constitutionality of cell tower dumps under the Fourth Amendment, including the lack of a consistent standard for obtaining cell tower dumps and the problems for law enforcement in requiring probable cause instead of specific and articulable facts.[42] Subsequently, in Part IV, this Note will argue that cell tower dumps do not constitute a search under the Fourth Amendment and are, therefore, subject to a standard of specific and articulable facts, a lesser standard than probable cause, in order to provide some privacy protection to individuals.[43]

II. CELL TOWER DUMPS AND THE FOURTH AMENDMENT: A BRIEF HISTORY

The Fourth Amendment of the United States Constitution, which governs searches and seizures, states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[44]

Throughout history, the U.S. Supreme Court has dealt with the question of what is a search.[45] Currently, there are no laws or Supreme Court decisions that directly address the issue of whether cell tower dumps are a search requiring probable cause.[46] Subpart A will discuss the

38. *See infra* Part IV.A.
39. *See infra* Part II.
40. *See infra* Part II.A.1–3.
41. *See infra* Part II.B.
42. *See infra* Part III.
43. *See infra* Part IV.
44. U.S. CONST. amend. IV.
45. *See infra* Part II.B.
46. *See* Owsley, *supra* note 9, at 2, 23 (explaining that there are no state or federal statutes addressing cell tower dumps and there are very few state or federal court cases addressing cell tower dumps); *see also* Press Release, Senator Edward Markey, For Second Year in a

legislation that is used to obtain cell tower dumps.[47] Subpart B will discuss Supreme Court cases concerning technology and the reasonable expectation of privacy under the Fourth Amendment.[48]

A. Legislative Initiatives Used to Obtain Cell Tower Dumps

As technology advances, Congress has passed some legislation to supply greater protections beyond those extended by the Fourth Amendment.[49] That being said, Congress has done very little to deal specifically with the issues created by cell tower dumps.[50] There are laws in place dealing with cell phone technology in general, but there are none that deal directly with cell tower dumps.[51] First, the Electronics Communications Privacy Act ("ECPA")[52] will be discussed below.[53] Next, this Note will investigate the Communications Assistance for Law Enforcement Act ("CALEA").[54] Finally, current proposed legislation on the topic of cell tower dumps will be explored.[55]

1. Electronics Communications Privacy Act

The ECPA seeks to deal with technologically advanced forms of communication, such as cell phones.[56] The ECPA "was designed to 'protect against the unauthorized interception of electronic

---

Row, Markey Investigation Reveals More than One Million Requests by Law Enforcement for Americans Mobile Phone Data (Dec. 9, 2014), *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 (discussing Senator Edward Markey's proposed legislation to protect American's cell-site location information).

47. *See infra* Part II.A.

48. *See infra* Part II.B.

49. Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications Act: Why Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 716 (2012). For example, Congress has passed the Electronics Communications Privacy Act, which includes the Stored Communications Act. *Id.* In 1994, Congress passed the Communications for Assistance of Law Enforcement Act, as well. *Id.* at 719.

50. *See* Press Release, Senator Edward Markey, *supra* note 46 (proposing legislation to curtail law enforcement access to information obtained via cell tower dumps).

51. GINA STEVENS ET AL., CONG. RESEARCH SERV., 7-5700, LEGAL STANDARD FOR DISCLOSURE OF CELL-SITE INFORMATION (CSI) AND GEOLOCATION INFORMATION 1, 2 (2010). There are four broad categories of surveillance in the area of electronic surveillance law: (1) wiretaps; (2) tracking devices; (3) stored communications and subscriber records; and (4) pen registers and trap-and-trace devices. *Id.*

52. 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2012).

53. *See infra* Part II.A.1.

54. 103 Pub. L. 414, 108 Stat. 4279 (1994); *see infra* Part II.A.2.

55. *See infra* Part II.A.3.

56. Harkins, *supra* note 8, at 1894.

communications.'"[57] It protects all communications—wired, oral, or electronic—while they are being made, are in transit, or are stored on a computer.[58] The Stored Communications Act ("SCA")[59] and the Pen Register Statute ("PRS") are components of the ECPA.[60]

The SCA details specific standards for law enforcement to obtain electronically stored data.[61] It governs law enforcement's right to use "stored user account information compiled by third parties in the ordinary course of business."[62] Congress's goal in passing the SCA was to protect individual privacy interests as technology expanded.[63] The SCA only applies to wire or electronic communications.[64] A wire communication is defined as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception."[65] Electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce . . . ."[66] Since the information obtained via cell tower dumps cannot be classified as a *wire* communication,[67] the SCA only governs cell tower dumps if they are classified as an *electronic* communication.[68]

When law enforcement requests information, the SCA divides the information sought into two mutually exclusive categories: (1) the substance of the communications; and (2) the records or subscriber/customer information.[69] However, the SCA does not allow

57. Owsley, *supra* note 9, at 13.

58. *Elec. Commc'ns Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, U.S. DEP'T OF JUST., https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last updated July 30, 2013) [hereinafter *ECPA*] (discussing that the ECPA is seen as an update on the Federal Wiretap Act—essentially, it applied the same principles from the Wiretap Act to electronic and digital communications).

59. *See generally* 18 U.S.C. §§ 2701–2712 (2012).

60. *See ECPA*, *supra* note 58; *see generally* §§ 3121–3127 (indicating the relevant sections of the U.S. Code that make up the Pen Register Statute).

61. *See* § 2703 (citing the relevant portion of the SCA that applies to cell-site location information); *see also* Elizabeth Elliot, Comment, United States v. Jones*: The (Hopefully Temporary) Derailment of Cell-Site Location Information Protection*, 15 LOY. J. PUB. INT. L. 1, 19 (2013).

62. Harkins, *supra* note 8, at 1896.

63. Elliot, *supra* note 61, at 19.

64. Chamberlain, *supra* note 21, at 1757.

65. *See* 18 U.S.C. § 2510(1) (2012).

66. *See* § 2510(12).

67. *See* § 2510(1), (12).

68. Chamberlain, *supra* note 21, at 1757.

69. *Id.* at 1755-56.

law enforcement to obtain records from a tracking device.[70] The main purpose of the SCA is to standardize government access to stored account information collected by a third party during the ordinary course of business.[71]

Importantly, the SCA permits the gathering of electronic communication records based on a showing of less than probable cause.[72] Currently, law enforcement can obtain cell tower data with a showing of specific and articulable facts.[73] The specific and articulable facts must show that "there are reasonable grounds to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[74] This places a lower burden on law enforcement than the burden created by probable cause.[75] The cell service provider must turn the information over without being required to provide notice to the subscriber or customer.[76]

The PRS, when first enacted in 1986, was narrowly defined.[77] However, following the passage of the USA PATRIOT Act,[78] the PRS was expanded to apply to wire and electronic communications as well as telephones.[79] It applies to two forms of telephone-based surveillance:[80] (1) pen registers;[81] and (2) trap-and-trace devices.[82] The PRS also

70. *Id.* at 1757-58; *see* 18 U.S.C. § 3117(b) (2012) (defining "tracking device" as "an electric or mechanical device, which permits the tracking of the movements of a person or object").

71. Harkins, *supra* note 8, at 1896.

72. Owsley, *supra* note 9, at 14.

73. Elliot, *supra* note 61, at 3, 19.

74. § 2703(d).

75. Owsley, *supra* note 9, at 15.

76. Elliot, *supra* note 61, at 19.

77. James McClintick, Comment, *Web Surfing in Chilly Waters: How The Patriot Act's Amendments to the Pen Register Statute Burden Freedom of Inquiry*, 13 AM. U. J. GENDER SOC. POL'Y & L. 353, 359-60 (2005) (explaining that when the PRS was first enacted the law was clear that law enforcement could only use pen registers to collect phone numbers dialed and sent over a telephone line); *see Surveillance Under the USA PATRIOT Act*, ACLU (Dec. 10, 2010), https://www.aclu.org/national-security/surveillance-under-usa-patriot-act. Following the passage of the USA PATRIOT Act the PRS was expanded to allow "nationwide pen register warrants" and to allow "pen register searches [to be] applied to the Internet." *Id.*

78. H.R. 3162, Pub. L. No. 107-56 (2001); *see also Surveillance Under the USA PATRIOT Act*, *supra* note 77 (explaining that the USA PATRIOT Act expanded Fourth Amendment exceptions "for spying that collects 'addressing' information about the origin and destination of communications, as opposed to the content").

79. Malone, *supra* note 49, at 720.

80. Chamberlain, *supra* note 21, at 1754-55.

81. 18 U.S.C. § 3127(3) (2014) (defining "pen registers" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication").

82. § 3127(4) (defining "trap-and-trace devices" as any "device or process which captures the

requires law enforcement to obtain a court order prior to installing such a device on a person's phone.[83] In order to obtain a court order, law enforcement officials must show that what they are requesting will be "relevant to an ongoing criminal investigation."[84] Although pen registers and trap-and-trace devices are often viewed as an archaic law enforcement investigatory technique, as a result of advances in technology, the PRS is still applicable to cell tower data because the government sometimes makes the argument that it is entitled to this information under the PRS.[85] Furthermore, the PRS "serves as the first watermark—the most permissive, purely legislative control over a form of electronic surveillance that does not constitute a Fourth Amendment search."[86]

2. Communications Assistance for Law Enforcement Act of 1994

Most recently, Congress passed the Communications Assistance for Law Enforcement Act of 1994 ("CALEA")[87] to aid law enforcement in obtaining cell phone data.[88] CALEA allows law enforcement officials to obtain location information only if it is achieved by obtaining cell phone numbers, precisely the function of a cell tower dump.[89] But, CALEA has limited this assistance, preventing law enforcement from obtaining location information under this law if it is attempting to obtain physical location information pursuant to the PRS.[90] CALEA requires cell service providers to guarantee that their equipment, facilities, and services allow access to "call-identifying information"—"dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a

---

incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

83. Chamberlain, *supra* note 21, at 1755.

84. Harkins, *supra* note 8, at 1895; *see also* § 3123(a)(1) (defining the standard of evidence the government must satisfy to obtain a PRS court order).

85. Harkins, *supra* note 8, at 1895 (explaining that law enforcement will sometimes combine the authority of the SCA, PRS, and CALEA when arguing they are entitled to cell tower dumps).

86. *Id.* at 1895-96.

87. 103 Pub. L. 414, 108 Stat. 4279 (1994).

88. Harkins, *supra* note 8, at 1899 (noting that "Congress's stated objective in passing the CALEA was to 'protect privacy in the face of increasingly powerful and personally revealing technologies'").

89. 47 U.S.C. § 1002(a)(2) (2014); Chamberlain, *supra* note 21, at 1758.

90. 47 U.S.C. § 1002(a)(2)(B) (2014) (explaining an exception in what sorts of information law enforcement can get using CALEA); Chamberlain, *supra* note 21, at 1758-59; Malone, *supra* note 49, at 719.

subscriber by means of any equipment, facility, or service of a telecommunications carrier."[91] Importantly, the call-identifying information cannot include information that would divulge the physical location of the customer, unless the location can be established from a telephone number.[92] Since wire communication and electronic communication are defined identically under CALEA and the SCA,[93] information from devices that are capable of tracking an individual's movements are not considered electronic communications under CALEA.[94]

3. Current Proposed Legislation

Recently, Senator Ed Markey[95] proposed new legislation that would make it more difficult for law enforcement to obtain cell phone information.[96] Under Senator Markey's bill, law enforcement would need a warrant to obtain Global Positioning System ("GPS") location data.[97] Additionally, the proposed legislation would limit cell service providers in terms of how long they could keep customers' phone data, and it would require law enforcement to disclose the nature and volume of requests made of cell service providers.[98]

The proposed legislation would not, however, necessitate a warrant for cell tower dumps.[99] Nevertheless, it would seek to restrain law

---

91. 103 Pub. L. 414, 108 Stat. 4279; *see also* 47 U.S.C. § 1001(2) (defining call-identifying information); Chamberlain, *supra* note 21, at 1759.

92. 47 U.S.C. § 1002(a)(2)(B); Chamberlain, *supra* note 21, at 1758-59. The relevant section of the PRS states:

> [W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) . . . .

§ 1002(a)(2)(B).

93. *See supra* notes 65-66 and accompanying text.

94. Chamberlain, *supra* note 21, at 1759.

95. *About Ed*, ED MARKEY U.S. SENATOR FOR MASS., http://www.markey.senate.gov/about (last visited Sept. 2, 2015).

96. Nakashima, *supra* note 9, at A8.

97. *Id.*; *see also* Press Release, Senator Edward Markey, *supra* note 46 (discussing that the proposed legislation would "[r]equire location tracking authorization only with a warrant when there is probable cause to believe it will uncover evidence of a crime" as is the same standard used by law enforcement to search a home).

98. Nakashima, *supra* note 9, at A8; *see also* Press Release, Senator Edward Markey, *supra* note 46 (explaining the proposed legislation would "[m]andate creation of rules by the Federal Communications Commission to limit how long wireless carriers can retain consumers' personal information").

99. Nakashima, *supra* note 9, at A8.

enforcement's ability to obtain such information by requiring that requests for cell tower dumps be more carefully modified.[100] Further, when the situation is an emergency, law enforcement authorities would need to provide a signed, sworn statement after receiving the information from a wireless service carrier to substantiate the request for emergency access.[101]

B. Supreme Court Cases Pertaining to Technology and Reasonable Expectation of Privacy Under the Fourth Amendment

To date, the Supreme Court has not decided whether cell tower dumps constitute a search under the Fourth Amendment.[102] However, the Supreme Court has dealt extensively with the Fourth Amendment and what does constitute a search.[103] Below, this Part will examine the Supreme Court case law regarding the Fourth Amendment and the reasonable expectation of privacy, the Third Party Disclosure Doctrine, and how it specifically relates to telephone usage.[104] An analysis of how the Supreme Court has applied the Fourth Amendment to advances in technology, from beepers to GPS tracking and cell phones, will follow.[105]

1. The Beginning of Fourth Amendment Jurisprudence

Current Fourth Amendment jurisprudence is based on the reasonable expectation of privacy test.[106] This test was established in 1967 when the Supreme Court decided *Katz v. United States*.[107] However, following the its decisions in *United States v. Miller*[108] and *Smith v. Maryland*,[109] the Court carved out some exceptions to the

100. Press Release, Senator Edward Markey, *supra* note 46 (explaining that the proposed legislation would seek to "[c]urb bulk data information requests such as cell tower dumps that capture information on a large group of mobile phone users at a particular period of time, and require that any request be more narrowly tailored").

101. *Id.* (discussing that the proposed legislation would "[r]equire, in the case of emergency circumstances, a signed, sworn statement from law enforcement authorities after receipt of information from a carrier that justifies the need for emergency access").

102. Malone, *supra* note 49, at 704; Adam Koppel, Note, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cell Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1072 (2010).

103. *See infra* Part II.B.1–3.

104. *See infra* Part II.B.1.

105. *See infra* Part II.B.2–3.

106. Steven Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J. L. & LIBERTY 556, 566 (2014).

107. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

108. 425 U.S. 435 (1976).

109. 442 U.S. 735 (1979).

reasonable expectation of privacy test—namely, assumption of the risk via the Third Party Disclosure Doctrine.[110]

In *Katz*, the Supreme Court made the radical change in Fourth Amendment doctrine to move from the *Olmstead v. United States*[111] trespass test[112] to the reasonable expectation of privacy test.[113] The Court held that "the Fourth Amendment protects people, not places."[114] However, the majority decision failed to sum up how those people would be protected and has become largely ignored.[115] Thus, the modern reasonable expectation of privacy test comes from Justice Harlan's concurrence: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[116] As a result of *Katz*, a warrant supported by probable cause is required not only for a physical search, but also for electronically collected information.[117]

The Supreme Court further defined Fourth Amendment jurisprudence in *United States v. Miller*.[118] In what has since become known as the Third Party Disclosure Doctrine, the Court held the Fourth

110. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1310, 1326-27 (2012).

111. 277 U.S. 438 (1928).

112. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding the Fourth Amendment only applied to physical searches where a trespass occurred). The Court determined that all the previous case law regarding the Fourth Amendment held that "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure," the Fourth Amendment will not be violated. *Id.* In this case, the Supreme Court held that wire-tapping did not constitute a search or a seizure within the meaning of the Fourth Amendment because there was no physical trespass. *Id.*; *see* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 1-2 (2009).

113. *See supra* note 31 and accompanying text.

114. Katz v. United States, 389 U.S. 347, 351 (1967) (explaining that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").

115. *Id.* at 359; *see* Winn, *supra* note 112, at 6.

116. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Many lower courts began to cite to Justice Harlan's concurring opinion, and after a year, the Court began using Justice Harlan's reasonable expectation of privacy test as the test for whether a search protected by the Fourth Amendment exists. Winn, *supra* note 112, at 7. Furthermore, within the decade that ensued, Justice Harlan's test had become so widely applied that the Supreme Court formally recognized it as the essence of *Katz*, which meant that the concurrence essentially replaced the majority in applicability and precedential value. *Id.*

117. Harkins, *supra* note 8, at 1888-89 (explaining that the Court left open to future decisions to determine exactly what types of electronic information gathering would involve the Fourth Amendment); *see infra* notes 118-63 (discussing Supreme Court cases where the Court has opined on the applicability of the *Katz* doctrine to new forms of technology).

118. 425 U.S. 435, 442-43 (1976).

Amendment does not apply to financial transaction records.[119] The Court reasoned that when a defendant "voluntarily conveys" the information sought by the government to third-party banks, the defendant assumes the risk of this information ending up in the hands of law enforcement.[120]

The Third Party Disclosure Doctrine was further extended in *Smith v. Maryland*.[121] The Supreme Court held that the installation of a pen register was not a Fourth Amendment search.[122] The Court reasoned that since pen registers only collect the numbers dialed from particular phones, they are minimally intrusive.[123] Most importantly, the Court found that since law enforcement was not gaining access to the content of the communications, but only the phone numbers dialed, pen registers do not violate a person's reasonable expectation of privacy.[124] Rather, the dialer assumed the risk that the telephone company will convey the phone numbers dialed to the government,[125] and a person does not have a reasonable expectation of privacy in the phone company's list of numbers dialed.[126]

---

119. *Id.* (discussing that all of the documents—including financial statements, deposit slips, and checks—obtained by the government "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"). Additionally, the Court argued that there can be no legitimate expectation of privacy in checks, because checks are "not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 442.

120. *Id.* at 443; *see* Chamberlain, *supra* note 21, at 1762; *see also* Mark Daniel Langer, Note, *Rebuilding Bridges: Addressing The Problems of Historic Cell Site Location Information*, 29 BERKLEY TECH. L.J. 955, 961-62 (2014) (explaining that the Court reasoned that since the bank was a party to the transaction then the bank was able to provide those records to the government).

121. 442 U.S. 735 (1979).

122. *Smith*, 442 U.S. at 741-42, 745-46 (arguing that since pen registers have such limited capabilities, they do not invade a persons reasonable expectation of privacy). Pen registers do not even allow law enforcement to ascertain whether a communication occurred; they merely alert law enforcement to when a phone number was dialed. *Id.* at 741.

123. Chamberlain, *supra* note 21, at 1762; *see* Marc C. McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 480 (2012) (analogizing the use of a pen register to collect telephone numbers dialed to searching the websites visited and e-mail addresses a person corresponds as both being minimally intrusive because, "neither technology acquires the contents of the communication at issue; rather, each technology reveals only the addressing information associated with the particular communication, where expectations of privacy are arguably diminished").

124. *See Smith*, 442 U.S. at 741-43 (explaining that pen registers cannot hear sound, so law enforcement does not obtain the content of any communications using pen registers); *see also* Chamberlain, *supra* note 21, at 1762-63 (discussing how it is unlikely that telephone users do not know that they are conveying the telephone number dialed to the phone company and even if they had an actual expectation of privacy it would not be reasonable because of the assumption of the risk doctrine).

125. *Smith*, 442 U.S. at 744; *see* Ohm, *supra* note 110, at 1326-27 (arguing that police power is expanded as a result of the assumption of the risk doctrine, allowing police to access records voluntarily conveyed to a third party without constitutional protections).

126. *Smith*, 442 U.S. at 745-46 (holding that a person generally lacks an actual expectation of

2. The Fourth Amendment and Advancing Technology

As technology advances, the Supreme Court has grappled with the applicability of the Fourth Amendment to new forms of technology.[127] Advances in technology often come with new ways for the government to invade an individual's reasonable expectation of privacy.[128] In *United States v. Knotts*,[129] the Supreme Court refused to extend Fourth Amendment protections when a beeper was used to track an individual on public streets.[130] The importance of the ruling in *Knotts* is that the Court exempted electronic surveillance from Fourth Amendment protection when the information obtained could also be observed through traditional surveillance techniques.[131]

However, in *United States v. Karo*,[132] the Court placed a significant limitation on the holding of *Knotts*.[133] In that case, police obtained information that could not have been achieved through visual observation.[134] The Court held that when law enforcement uses tracking devices to obtain information that would otherwise be shielded from the public, a warrant supported by probable cause is required under the Fourth Amendment.[135] When the holdings of *Knotts* and *Karo* are combined they "establish a 'public/private dichotomy' that governs the Fourth Amendment validity of law enforcement use of tracking devices."[136]

---

privacy in the telephone numbers dialed and even if that person had an actual expectation of privacy in the telephone numbers dialed, it would not be a legitimate expectation of privacy).

127. *See infra* notes 128-63 and accompanying text.

128. *See* Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?*, 2011-2012 CATO SUP. CT. REV., 26, 27, http://object.cato.org/sites/cato.org/files/serials/ files/supreme-court-review/2012/9/scr-2012-kozinski-nguyen.pdf (discussing the impact of advancements in technology and the Fourth Amendment).

129. 460 U.S. 276 (1983).

130. *Knotts*, 460 U.S. at 281-82 (holding a person cannot have a reasonable expectation of privacy on public streets); *see also* Marc C. McAlister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207, 215 (2014) (explaining the using the beeper to track the defendant was not a Fourth Amendment search because "the beeper did not provide any information police could not have obtained through visual surveillance along the vehicle's route").

131. Harkins, *supra* note 8, at 1890.

132. 468 U.S. 705 (1984).

133. Chamberlain, *supra* note 21, at 1765.

134. *Karo*, 468 U.S. at 707, 714; *see* McAlister, *supra* note 130, at 215-16 (discussing how the Court in *Karo* reached the opposite result because the beeper was used to track the defendant's movements inside a private residence).

135. *Karo*, 468 U.S. at 716 (reasoning that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight"); Harkins, *supra* note 8, at 1890.

136. Chamberlain, *supra* note 21, at 1767.

The Court further expanded Fourth Amendment protections in areas of technological advancement in *Kyllo v. United States*.[137] The Supreme Court sought to protect individuals from governmental intrusion when police used sensory enhancing technology, which was not available to the general public, to gain access to parts of a home that could not be seen without "physical intrusion."[138] The Court articulated that the surveillance conducted in this case was considered a search and was unreasonable without a warrant.[139] Thus, the general rule regarding advancing technology appears to be that, as long as the technology is accessible to the public, law enforcement can use it without a warrant.[140] As a result, law enforcement cannot use the latest technology, which assures that citizens retain the "degree of privacy against the government that existed when the Fourth Amendment was adopted," before the invention of the new technology.[141]

Recently, the Court was asked to determine whether prolonged GPS tracking of a person's vehicle was a violation of the Fourth Amendment.[142] In *United States v. Jones*,[143] the Supreme Courtheld that police physically trespassed onto private property by putting a GPS on the car, and therefore the use of GPS tracking was a search.[144] Following the Court's ruling, the Fourth Amendment can be violated if it is shown that law enforcement trespassed or violated a person's reasonable expectation of privacy.[145]

---

137. 533 U.S. 27 (2001).

138. *Id.* at 34-35. Police suspected the defendant of growing marijuana in his home so they used a thermal imager to detect heat levels. *Id.* at 29-30. Law enforcement officers scanned the home from a vehicle across the street from the house and the scan only took a couple of minutes. *Id.*

139. *Id.* at 34 (holding that where the information is obtained using "sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use").

140. *Id.* at 34-35 (explaining that the use of the thermal imager in this case was a search when it was examined against the criteria discussed above); *see* Ohm, *supra* note 110, at 1328.

141. *Kyllo*, 533 U.S. at 34 (reasoning that the holding assured "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"); *see* Sutton, *supra* note 1, at 267-68.

142. *See* United States v. Jones, 132 S. Ct. 945, 948 (2012). *But see* People v. Weaver, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009) (applying a Mosaic Theory approach to determine if GPS tracking was a search under the New York State Constitution). The court reasoned: "Here, we are not presented with the use of a mere beeper to facilitate visual surveillance during a single trip. GPS is a vastly different and exponentially more sophisticated and powerful technology that is easily and cheaply deployed and has virtually unlimited and remarkably precise tracking capability." *Id.* at 1199.

143. 132 S. Ct. 945 (2012).

144. *Id.* at 949.

145. Bellovin et al., *supra* note 106, at 569-70.

As Justice Sotomayor points out in her concurrence, police used GPS to track the defendant's movement for four weeks.[146] Justice Sotomayor acknowledged that the trespass test cannot provide the required direction for determining Fourth Amendment cases where new forms of technology are involved.[147] She disagreed with the use of GPS tracking for both long-term and short-term monitoring because it is unique when she noted that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familiar, political, professional, religious, and sexual associations."[148] Justice Sotomayor also argued that the Court needs to reconsider the applicability of the Third Party Disclosure Doctrine in the digital age because people expose a lot of private information about themselves via technology.[149] Instead, she proposed that the Mosaic Theory[150] should be applied in the digital age because if the Court continues to follow the Third Party Disclosure Doctrine, the government can get a whole picture of a person's life without any restrictions.[151] Justice Sotomayor reasoned that the Mosaic Theory should cover a search where law enforcement learns details about a

146. *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring).

147. Elliot, *supra* note 61, at 17.

148. *Jones*, 132 S. Ct. at 955; *see* Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2013-2014 CATO SUP. CT. REV. 307, 317.

149. *Jones*, 132 S. Ct. at 957.

150. *See* United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010) (applying the Mosaic Theory in deciding the lower court case *Jones* was appealed from); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012). The Mosaic Theory necessitates that the Fourth Amendment search doctrine is applied to government actions in their entirety, not just to the isolated steps. Kerr, *supra*. Rather than asking if a specific act is a search, "the Mosaic Theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group." *Id.* In *Maynard*, the court determined that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble." 615 F.3d at 562. This information combined can reveal more about a person than any individual trip does in isolation. *Id.*; Kerr, *supra*, at 326. The court reasoned that month-long surveillance of a person's movements, which were not exposed to the public, is similar to a rap sheet because it reveals much more than just the person's movements. *Maynard*, 615 F.3d at 561-62. Further, the court felt that twenty-eight days worth of surveillance was a search under the Fourth Amendment because it exposed an intimate look into an individual's life that "he expects no one to have–short perhaps of his spouse." *Id.* at 563. The problem is not the level of intrusion, but rather the kind of intrusion because "no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life" *Id.* at 562. The majority in *Maynard* suggests the Mosaic Theory should be applied when the government search reveals "more than a stranger could have observed." *See* Kerr, *supra*, at 330. Numerous nonsearches combined, become a search "because the individual pieces of the puzzle that seemed small in isolation could be assembled together like a mosaic to reveal the full picture of a person's life." *Id.* at 325.

151. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

person's life "more or less at will," meaning that they can access nearly all facets of a person's life without her knowledge.[152]

Justice Alito's concurrence calls for the application of Fourth Amendment search restrictions when law enforcement conducts long-term GPS tracking of a suspect, but would not require a warrant for short-term GPS tracking.[153] Applying the traditional *Katz* reasonable expectation of privacy test, he reasoned that the four weeks of GPS monitoring conducted in this instance constituted a length of time that violated the Fourth Amendment.[154] Justice Alito argued that the Mosaic Theory should be applied to a search where "investigators collect and analyze evidence in a way that would surprise members of society."[155] The difficulty presented by Justice Alito's application of the Mosaic Theory is that it provides relatively little guidance for law enforcement and judges about when Fourth Amendment issues arise because his application does not examine what sorts of investigations might surprise society.[156]

3. The Fourth Amendment and Cell Phone Technology

The Supreme Court recently recognized the need to address the Fourth Amendment implications for cell phone technology.[157] In *Riley v. California*,[158] the Court reviewed two cases in which police searched

152. Kerr, *supra* note 150, at 330.

153. *Id.* at 327.

154. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

155. Kerr, *supra* note 150, at 330; *see also Elec. Commc'ns Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H.R. Comm. on the Judiciary*, 113th Cong. 105 (2013) [hereinafter *ECPA Hearing*] (materials submitted by Representative Scott). When analyzing Justice Alito's concurring opinion in *Jones* one scholar noted:

> The Alito concurrence posits 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' while law enforcement secretly monitor[ing] and catalogu[ing] every single movement of an individual's car for a very long period does not accord with reasonable expectations of privacy.

ECPA Hearing, *supra*.

156. *ECPA Hearing*, *supra* note 155, at 106 (explaining that the line of demarcation as to when the GPS tracking became a search is unclear because while the Majority argues that four weeks was "surely too long," Justice Alito believes the GPS tracking became a search before it reached the four week mark, even though he never states specifically when he feels the GPS tracking became a search).

157. *See* Pincus, *supra* note 148, at 321; *see also Supreme Court Watch: Ten Key Issues From the* Riley *Opinion Protecting Cell Phone Data Seized During an Arrest*, FED. EVID. BLOG (June 30, 2014), http://federalevidence.com/blog/2014/june/supreme-court-watch-cell-phone-content-protected-under-fourth-amendment.

158. 134 S. Ct. 2473 (2014).

suspects' cell phones without warrants.[159] The Court held that before law enforcement could search a person's cell phone, they must obtain a warrant.[160] The majority opinion stated: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[161] Additionally, a person's cell phone contains, in "digital form, many sensitive records previously found in the home [and] it also contains a broad array of private information never found in a home in any form—unless the phone [itself was in the home]."[162] Therefore, in order to protect a person's privacy, the Court required law enforcement to obtain a warrant before searching a person's cell phone.[163]

159. *Id.* at 2480-82 (discussing the two cases, which were combined); Pincus, *supra* note 148, at 321-22. In the first case, the defendant was stopped for driving with expired registration tags. *Riley*, 134 S. Ct. at 2480. He was arrested, and, during the search incident to arrest, police seized a cell phone. *Id.* The officer went through the phone and noticed some language he took to mean the defendant was a member of the Bloods, a notorious street gang. *Id.* At the police station, another officer went through the phone and found a picture of the defendant standing in front of a car police believed was involved in a shooting weeks earlier *Id.* at 2581. In the second case, police saw the defendant making a drug deal. *Id.* Police arrested the defendant and seized two cell phones. *Id.* While at the police station, one phone was repeatedly getting phone calls from "my house." *Id.* Police opened the phone and saw a picture of a woman and baby as the phone's background. *Id.* Police accessed the phone book and looked up the number associated with "my house" and were able to use that to find the defendant's home address, which they subsequently searched and found drugs, weapons, and money. *Id.*

160. *Riley*, 134 S. Ct. at 2485; *see* Adam Liptak, *Justices, 9-0 Rule Cellphone Search Needs a Warrant*, N.Y. TIMES, June 26, 2014, at A1 (describing the significance of this decision with regards to its likely impact on other forms of technology); *see also* John Schwartz, *Cellphone Ruling Could Alter Police Methods, Experts Say*, N.Y. TIMES, June 26, 2014, at A18 (explaining that the message from the Supreme Court to law enforcement is clearly to "get a warrant" when searching a cell phone).

161. *Riley*, 134 S. Ct. at 2489; *see* Adam Lamparello and Charles MacLean, Riley v. California*: The New* Katz *or* Chimel*?*, 21 RICH. J.L. & TECH. 1, 3 (arguing that the Supreme Court's holding in *Riley* suggests the Court views "cellular telephones, particularly smartphones, along with laptop computers and other digital devices, [as] the twenty-first century's private 'homes,' where individuals store the 'papers and affects' traditionally accorded Fourth Amendment protection").

162. *Riley*, 134 S. Ct. at 2491; *see* Pincus, *supra* note 148, at 325 (meaning that when police search a cell phone they often have greater access to ordinarily unavailable personal information).

163. *Riley*, 134 S. Ct. at 2485; *see* Pincus, *supra* note 148, at 325 (explaining the Court balanced the impact on a legitimate expectation of privacy with the effects of the search incident to arrest exception determining "that the exception does not apply to digitally stored information contained in a device seized in the course of an arrest" to reach the conclusion that a warrant was necessary).

III. PROBLEMS WITH DETERMINING THE CONSTITUTIONALITY OF CELL TOWER DUMPS UNDER THE FOURTH AMENDMENT

In general, it is difficult to determine the constitutionality of searches under the Fourth Amendment.[164] Advances in technology have not made this an easier task.[165] As technology changes and improves, questions of a person's reasonable expectation of privacy become unclear.[166] In today's world, it is not uncommon for a person's cell phone or computer to contain more private information than can be found in the remainder of her home, because of the vast amount of personal information that can be stored on a cell phone.[167] This makes the task of determining a concrete rule regarding the constitutionality of cell tower dumps difficult for the legislature or the courts.[168] There are several occasions where the use of cell tower dumps can be extremely beneficial to law enforcement.[169] If they were required to obtain a warrant before getting the data, valuable time would be lost.[170] Adopting a probable cause standard for cell tower data, which is less precise than GPS location data, would severely hamper law enforcement efforts.[171]

Inconsistencies in cell tower legislation have led to confusion for law enforcement.[172] Below, this Part will explore the inconsistencies created by the lower federal courts with regard to the standard necessary to obtain cell tower dumps.[173] Furthermore, this Part will discuss the

164. *See supra* Part II.B.

165. *See supra* Part II.B.

166. *See* Kozinski & Nguyen, *supra* note 128, at 15-16 (discussing how technology has changed the way the Fourth Amendment must be examined).

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

168. Kozinski & Nguyen, *supra* note 128, at 16.

169. *ECPA Hearing*, *supra* note 155, at 20 (statement of Peter A. Modafferi). In one case in particular, law enforcement used cell tower dumps in a robbery case in Rockland County, New York. *Id.* There were seven bank robberies in the area and police were unable to find any suspects until a witness—a victim in one of the robberies—showed them photographs of the suspect's car. *Id.* Law enforcement obtained a subpoena and tried to figure out who purchased the car. *Id.* Law enforcement then issued another subpoena for the basic subscriber information and phone numbers—a cell tower dump. *Id.* Using the information from the cell tower dump, law enforcement obtained a court ordered subpoena for historical cell-site location information. *Id.* Law enforcement then used the information obtained from this to request a trap-and-trace pen register with location authorization. *Id.* The information received from this device provided law enforcement with the probable cause necessary to use GPS tracking, which ultimately resulted in the arrest of the robbery suspects immediately after their next robbery. *Id.*

170. *Id.*

171. *Id.*

172. *See infra* Part III.A.

173. *See infra* Part III.B.

issues that would be created for law enforcement officials by requiring them to show probable cause at this stage.[174]

A. Lack of Clarity on What Standard Is Necessary to Obtain Cell Tower Dumps Has Led to Inconsistencies for Law Enforcement

Since there is no legislation dealing directly with cell tower dumps, law enforcement must rely on legislation dealing with cell phone technology in general.[175] The inconsistent standards among the SCA, the PRS, and CALEA have created confusion for law enforcement.[176] Inconsistent decisions by the lower courts as to what standard is necessary to obtain the information creates further confusion for law enforcement regarding the constitutionality of cell tower dumps.[177] The lower courts have interpreted the applicability of the various pieces of legislation dealing with cell tower dumps differently and, as a result, law enforcement does not have clear instruction of what is necessary to obtain a cell tower dump.[178] Due to this lack of clarity, there is little guidance on which law to apply when requesting cell tower dumps.[179] Law enforcement is left free to interpret the laws and court decisions in whatever fashion they prefer to obtain the cell tower dumps.[180]

One of the greatest challenges for law enforcement seeking cell tower dumps is determining the appropriate legal standard to apply.[181] There is no legislation that directly addresses the legal standard necessary to acquire cell tower dumps.[182] Law enforcement and the

174. *See infra* Part III.C.

175. Owsley, *supra* note 9, at 2, 43; *see supra* Part II.A.

176. *See* Harkins, *supra* note 8, at 1887 (explaining that the core of the dispute surrounding what standard governs cell tower dumps is what statute governs the disclosure); *see supra* notes 73-74 and accompanying text (discussing the SCA standard to obtain cell tower data); *supra* notes 83-84 and accompanying text (discussing the PRS standard to obtain cell tower data); *supra* note 91 and accompanying text (discussing CALEA standard to obtain cell tower data).

177. *ECPA Hearing*, *supra* note 155, at 96 (explaining that the courts have created an "inconsistent legal landscape" by reaching different conclusions regarding the constitutionality of cell tower dumps); *see infra* Part III.C.

178. *See ECPA Hearing*, *supra* note 155, at 96 (arguing that the system that has been created "neither serves law enforcement needs nor protects privacy interests," because too much uncertainty has been created); *see infra* Part III.C.

179. *See* Harkins, *supra* note 8, at 1887 (explaining the confusion created in the application of the various statues typically used to obtain cell tower dumps); *ECPA Hearing*, *supra* note 155, at 96 (discussing the confusion lower federal courts have created regarding cell tower dumps); *see supra* notes 175-78 and accompanying text; *infra* notes 180-209 and accompanying text.

180. *See* Chamberlain, *supra* note 21, at 1768-69 (explaining that law enforcement created a hybrid theory for obtaining cell-site information by combining the various standards from legislation in order to convince the court to grant the order).

181. *ECPA Hearing*, *supra* note 155, at 35 (statement of Catherine Crump).

182. Crusco, *supra* note 13, at 5.

courts have interpreted the SCA, the PRS, and CALEA as being applicable but have not agreed on how these statutes apply.[183] Adding to this challenge is the fact that the SCA, the PRS, and CALEA all require different standards to obtain cell tower dumps.[184] The lack of clarity among the various statutes used to obtain cell tower dumps results in law enforcement using creative means to obtain the information they seek.[185]

Since the SCA is only applicable to wire or electronic communications, and information obtained via cell tower dumps is not classified as a wire communication,[186] the SCA can only govern cell tower dumps if they are classified as an electronic communication.[187] The SCA protects information by: (1) "limit[ing] the government's ability to compel private communications companies to disclose information about subscribers;" and (2) "limit[ing] a private company's ability to voluntarily turn over information about a subscriber to the government."[188] Importantly, the SCA permits law enforcement to gather electronic communication records based on a showing of less than probable cause.[189] Currently, under the SCA, law enforcement officials can obtain cell tower dumps with a showing of specific and articulable facts.[190]

Law enforcement most frequently invokes section 2703(d) of the SCA as its means of obtaining cell tower dumps.[191] The provision is generally considered a less stringent standard than is required to obtain a warrant.[192] SCA section 2703(d) provides:

> A court order for disclosure under subsection (b) or (c) . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire of electronic communication, or the records or other

183. *See infra* Part III.B.

184. *See supra* notes 175-83 and accompanying text; *infra* notes 185-209 and accompanying text.

185. *See infra* notes 204-09 and accompanying text (discussing law enforcement's use of a hybrid theory to obtain cell tower dumps).

186. 18 U.S.C. § 2510(1) (2014) (defining "wire communications" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception"); § 2510(12) (defining "electronic communication" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications"); Chamberlain, *supra* note 21, at 1757.

187. Chamberlain, *supra* note 21, at 1757.

188. Malone, *supra* note 49, at 716-17.

189. Owsley, *supra* note 9, at 14.

190. *See* Elliot, *supra* note 61, at 3; *see also* Owsley, *supra* note 9, at 30.

191. Elliot, *supra* note 61, at 19.

192. Chamberlain, *supra* note 21, at 1757.

> information sought, are relevant and material to an ongoing criminal investigation.[193]

Confusion arises, however, because the SCA does not permit the government to obtain information from a device that could be used to track a person's movements, even if it is a form of electronic communication.[194] Because a cell phone is capable of being used as a tracking device, there is often a misunderstanding as to whether the SCA's specific and articulable facts standard is applicable.[195]

The PRS requires law enforcement to obtain a court order prior to installing a pen register or a trap-and-trace device on a person's phone.[196] In order to obtain a court order to install such a device, the PRS requires law enforcement to show that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[197] Law enforcement seeks creative alternatives to obtain cell tower dumps by indirectly applying the PRS.[198] Additionally, following the USA PATRIOT Act expansions of the PRS, the Fourth Amendment exceptions "for spying that collects 'addressing' information about the origin and destination of communications, as opposed to the content," were applied to cell tower dumps.[199] Significantly, following the passage of the USA PATRIOT Act, the government can gain access more easily to records of the activities of private citizen's held by third parties.[200]

CALEA provides law enforcement with the greatest success of achieving their goal of obtaining a cell tower dump because it allows law enforcement to obtain location information when all it gets is cell phone numbers.[201] However, when law enforcement is seeking call-identifying information solely pursuant to authority given under the PRS, the call-identifying information cannot include any information that could

193. 18 U.S.C. § 2703(d) (2014).

194. Chamberlain, *supra* note 21, 1758.

195. *Id.* at 1757-58; *see also* Owsley, *supra* note 9, at 30 (explaining that although § 2703(d) of the SCA requires specific and articulable facts, a magistrate could require a showing of probable cause if he or she feels it is necessary even when the information law enforcement officials are requesting would not result in tracking a person via their cell phone, removing the solidity of the § 2703(d) standard).

196. Chamberlain, *supra* note 21, at 1755.

197. 18 U.S.C. § 3123(a)(1) (2014) (defining the standard of evidence the government must satisfy to obtain a PRS court order); Harkins, *supra* note 8, at 1895.

198. Harkins, *supra* note 8, at 1901 (explaining how the government combines elements of the SCA, the PRS, and CALEA to create a hybrid theory to obtain cell-site location information).

199. H.R. 3162, Pub. L. No. 107-56 § 214; *see Surveillance Under the USA PATRIOT Act*, *supra* note 77.

200. *Surveillance Under the USA PATRIOT Act*, *supra* note 77.

201. Chamberlain, *supra* note 21, at 1758.

disclose the physical location of the person.[202] Significantly, since "the terms 'wire communication' and 'electronic communication' are defined in the same way under CALEA as they are under SCA, communications from devices that can be used to track an individual's movements are not 'electronic communications' under CALEA."[203]

The competing nature of the various cell tower dump statutes makes it relatively easy to see why law enforcement officials would seek to acquire cell tower dumps using a hybrid theory.[204] In applying a hybrid theory, government officials request the information sought using the most favorable parts of the SCA, the PRS, and CALEA.[205] In effect, law enforcement officials create their own "law" that is tailor-made and under which they can have nearly unlimited access to cell tower dumps.[206] When the government seeks to obtain a cell tower dump using the hybrid theory

> [t]he statutory argument [it] claim[s is] that the [PRS] permits the capture of numbers for incoming and outgoing calls, and that when used on cellular phones these devices would also disclose [location information] at the beginning and end of each call. Next, the government cite[s] CALEA as requiring that the courts rely also on some additional statutory authority when ordering the disclosure of [real-time] cell-site information under the [PRS], and contend[s] that this additional authority was provided under the SCA.[207]

In essence, this hybrid theory makes it much easier for the government to get information using cell tower dumps because it has applied the most favorable parts of the cell tower statutes, which means that it can obtain this information under the lower standard of specific and articulable facts.[208] However, the government has had little success in applying this hybrid theory, mainly because courts view it as an unwarranted reading of the applicable statutes.[209]

202. Malone, *supra* note 49, at 719.
203. Chamberlain, *supra* note 21, at 1759.
204. Harkins, *supra* note 8, at 1895, 1901.
205. *Id.* at 1901.
206. *Id.*
207. *Id.* (internal quotation marks omitted).
208. Chamberlain, *supra* note 21, at 1768-69.
209. *Id.* at 1769-73.

B. *Lack of Clarity from Lower Federal Courts on What Standard Is Necessary to Obtain Cell Tower Dumps Has Led to Inconsistencies for Law Enforcement*

The lower federal courts appear to be somewhat unpredictable on the standard they will indicate is necessary to obtain a court order to conduct a cell tower dump.[210] Some lower federal courts have applied the SCA § 2703(d) specific and articulable facts standard, whereas others have determined probable cause is necessary to obtain a warrant for cell tower dumps under the Fourth Amendment.[211] This has created confusion for law enforcement seeking cell tower dumps.[212]

Several lower federal courts have held that the specific and articulable facts standard of SCA § 2703(d) is the correct standard to be applied when deciding whether or not to grant a subpoena for cell-site location data.[213] The Third Circuit held specific and articulable facts means that law enforcement must show "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."[214] The court examined the legislative history, determining that neither the SCA itself nor its legislative history dictates that the government must show probable cause to obtain cell-site location data.[215]

In a recent case decided on the issue, a district court judge in New York held that a warrant was not required because the information requested—the telephone numbers—were voluntarily disclosed, and thus, the information did not implicate the same privacy concerns as would be generated if the content of the communications was sought.[216]

---

210. *See infra* notes 211-30 and accompanying text.

211. *See infra* notes 213-26 and accompanying text (discussing lower courts which support the specific and articulable facts standard), notes 227-30 (discussing lower courts which support the probable cause standard).

212. *See infra* Part III.C.

213. *In re* U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (holding the government could obtain cell-site information using 18 U.S.C. § 2703(d), which does not require probable cause); *In re* United States, 42 F. Supp. 3d 511, 512-14, 519-20 (S.D.N.Y. 2014) (holding all that was needed was an order under 18 U.S.C. § 2701(d) and that cell tower dumps were not a Fourth Amendment search because of the Third Party Disclosure Doctrine); *In re* U.S. Orders Pursuant to 18 U.S.C. 2703(d), 509 F. Supp. 2d 76, 81-82 (D. Mass. 2007), *rev'd*, 509 F. Supp. 2d 64 (D. Mass. 2007) (holding the only standard necessary is that the request be supported by "specific and articulable facts").

214. *In re U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 313; *see also* Owsley, *supra* note 9, at 30 (explaining that the Third Circuit leaves to the discretion of the magistrate whether or not to require probable cause).

215. *In re U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't.*, 620 F.3d at 315.

216. *In re United States*, 42 F. Supp. 3d at 519 (requiring the government to amend their

The district court determined that cell tower dumps do not violate a person's Fourth Amendment protection against unreasonable searches and seizures so they do not require a warrant.[217] The opinion stated that law enforcement wanted phone numbers used during a given period, in a given location, which were to be cross-referenced with other information law enforcement had gathered throughout the investigation.[218] Therefore, cell tower dumps do not afford the Government the possibility of tracking people as a result of the authorization of a cell tower dump.[219] Furthermore, the court applied the Third Party Disclosure Doctrine, stating that subscribers are aware that the use of a cell phone necessitates the disclosure of the information sought via cell tower dumps.[220] The court concluded that although some government searches of voluntarily disclosed information might be so invasive that a showing of probable cause would be required, the case of cell tower dumps is not one of those cases.[221] This is because "the telephone numbers associated with the communications in a general location do not implicate privacy interests to the same degree as . . . the content of those communications."[222]

In another recent case regarding cell tower dumps, a magistrate judge in Texas granted an order compelling a cell tower dump using the SCA.[223] Law enforcement requested "seven different cell phone service providers to release historical cell tower data for specific towers providing service to a crime scene within Houston city limits at the hour of the crime."[224] Law enforcement did not specify a phone number or specific identity of a suspect they were targeting.[225] The district court reasoned the SCA § 2701(d) standard of specific and articulable facts was properly applied in this case and authorized the cell tower dump.[226]

Alternatively, a number of lower federal courts held that in order to request historical cell-site location data law enforcement must show

---

request to "(1) provide[ ] more specific justification for the time period for which the records will be gathered and (2) outline a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved").

217. Mark Hamblett, *After Seeking ACLU Views, Judge Approves 'Cell Tower Dump,'* 251 N.Y. L.J. 1, 1 (2014).

218. *In re United States*, 42 F. Supp. 3d at 515.

219. *Id.*

220. *Id.* at 517-18.

221. *Id.* at 519.

222. Hamblett, *supra* note 217, at 6.

223. *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), No. H–15–136M, 2015 WL 1022018, at *1 (S.D. Tex. March 9, 2015).

224. *Id.*

225. *Id.* (explaining it was the hope of law enforcement that by using the cell tower data a suspect could be identified and arrested).

226. *Id.* at *4-5 (holding the only restriction placed on law enforcement's request was to limit the temporal scope from one hour to ten minutes).

probable cause.[227] Although not all courts held a warrant was necessary, they have determined that a court order to obtain such information would not be granted without a showing of probable cause.[228] In one case a court held that "existing Fourth Amendment doctrine must be interpreted so as to afford constitutional protection to the cumulative cell-site location records requested here."[229] The court reasoned that if it were to apply the Third Party Disclosure Doctrine to cumulative cell-site location data it would allow law enforcement to intrude into information "objectively recognized as highly private."[230]

C. *Problems for Law Enforcement in Requiring Probable Cause for Cell Tower Dumps*

There can be little argument that the use of cell tower dumps provides a helpful and efficient investigative tool for law enforcement.[231] One law enforcement officer explained: "Geolocation information is an essential building block in 'the construction' of a criminal investigation."[232] The problem with requiring probable cause for cell

227. *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2701(d), 964 F. Supp. 2d 674, 677-78 (S.D. Tex. 2013) (holding that the government needed a warrant for the information requested and that they did not have sufficient evidence of probable cause to support the granting of the warrant); *In re* Search of Cellular Tel. Towers, 945 F. Supp. 2d 769, 770-71 (S.D. Tex. 2013) (granting the warrant to obtain information as a result of cell tower dumps because it was supported by probable cause); *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Location Records, 930 F. Supp. 2d 698, 701 (S.D. Tex. 2012) (denying the order because the statute relied upon by the government did not address cell tower dumps and cell tower dump records can only be obtained with a showing of probable cause); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (denying the government's application because people have a reasonable expectation of privacy in long-term cell-site location records).

228. *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 596 (E.D.N.Y 2010) (denying the government's request for historical cell-site location data because the court held probable cause was required under the Fourth Amendment); *In re* U.S. *ex rel.* Historical Cell Site Data, 747 F. Supp. 2d 827, 836-40, 846 (S.D. Tex. 2010) (using *Karo* and *Maynard*, the court denied the government's request for cell-site information because the government failed to show the location of the user was voluntarily conveyed in the data requested); *In re* Application of the U.S., 727 F. Supp. 2d 571, 583-84 (W.D. Tex. 2010) (holding the cell phones were tracking devices and, therefore, cell-site location information constitutes a search under the Fourth Amendment).

229. *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 127.

230. *Id.* at 126; *see also* United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014), *aff'd* 785 F.3d 498 (11th Cir. 2015) (en banc) (holding that obtaining a cell tower dump under the SCA was not a search, and that, even if it was, obtaining the cell phone records without a warrant was reasonable).

231. Owsley, *supra* note 9, at 23 (calling cell tower dumps "a valuable weapon in law enforcement's arsenal").

232. *ECPA Hearing*, *supra* note 155, at 27 (statement of Peter A. Modafferi).

tower dumps is that when law enforcement seeks to conduct a cell tower dump, they do not have a suspect they are targeting.[233] The Federal Bureau of Investigation ("FBI") commonly uses cell tower dumps in the early stages of robbery investigations to help identify suspects.[234] In the first case where the FBI used a cell tower dump to find bank robbers, FBI Agents used cell tower dump records that corresponded with the area and time of nearly a dozen bank robberies committed by the "Scarecrow Bandits."[235] The records showed two of the suspected Scarecrow Bandits' cell phones connected to cell towers in the vicinity of the bank robberies at or around the time they were committed.[236] The FBI used the cell tower dump records to link the cell phones of two of the defendants to other members of the Scarecrow Bandits group whose cell phones were also linked to cell towers near the robbery locations.[237] Once the FBI identified suspects in the bank robberies, they were able to focus their investigation on these individuals allowing the FBI to conduct visual surveillance to prevent future bank robberies.[238] In another bank robbery case, the FBI used cell tower dumps to arrest the "High Country Bandits."[239] The FBI received information from a witness at one of the bank robberies that a couple of hours before the robbery occurred, a suspicious looking man was outside the bank talking on a cell phone.[240] Using this tip, the FBI sought to get a cell tower dump to identify a common cell phone number near all of the bank robberies.[241] In this case, "the FBI asked a federal magistrate judge to approve four of these cell tower dumps [in the] four most rural [robbery] locations in order to minimize the amount of extraneous telephone data that would likely be obtained."[242] Agents obtained over 150,000 telephone numbers, which they cross-referenced to find common numbers at the crime scenes.[243] These cases illustrate that law

233. *Id.* at 22 (statement of Peter A. Modafferi); Crusco, *supra* note 13, at 5.

234. *See* United States v. Duffey, No. 3:08-CR-0167-B, 2009 WL 2356156, at *1 (N.D. Texas July 30, 2009); *see also* Anderson, *supra* note 10.

235. *Duffey*, 2009 WL 2356156, at *1; *see also* Owsley, *supra* note 9, at 25 (explaining that the Scarecrow Bandits were a group of armed robbers that "violently robbed more than twenty banks in the Dallas area").

236. *Duffey*, 2009 WL 2356156, at *1; *see also* Owsley, *supra* note 9, at 25.

237. Brian L. Owsley, *Cops and Robbers: The Use of Cell Tower Dumps to Investigate Bank Robberies*, AM. CRIM. L. REV. BLOG: MENS REA, (Jan. 26, 2013), http://www.americancriminallawreview.com/aclr-online/cops-and-robbers-use-cell-tower-dumps-investigate-bank-robberies.

238. *Duffey*, 2009 WL 2356156, at *2.

239. Anderson, *supra* note 10.

240. *Id.*

241. *Id.*

242. *Id.*

243. Owsley, *supra* note 9, at 27. The judge dismissed the defendant's argument that a cell

enforcement uses cell tower dump data to help establish probable cause at the beginning of an investigation when they have little evidence to go off of.[244]

Another example of the effectiveness of cell tower dumps as an investigative tool is that it now takes U.S. Marshalls only two days to find a fugitive, compared to the forty-two days it used to take.[245] The Associate Deputy Attorney General told a Senate Committee that "if an amendment [to the ECPA] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost."[246] It is the opinion of Peter Modaferri, Chief of Detectives at the Rockland County, New York, District Attorney's Office, that "[r]equiring probable cause to get basic, limited information about a person's historical location would make it significantly more difficult to solve crimes and seek justice."[247]

IV. THE SPECIFIC AND ARTICULABLE FACTS STANDARD SHOULD BE UNIVERSALLY APPLIED TO CELL TOWER DUMPS

Cell tower dumps are not considered a search under the Fourth Amendment.[248] Since law enforcement acquires only a suspect's cell phone number, no search is conducted, and therefore, no Fourth Amendment right is hindered.[249] Further, when law enforcement requests a cell tower dump, it does not have a specific suspect it is targeting.[250] Therefore, law enforcement should not be subjected to a required showing of probable cause and should not need to obtain a warrant before obtaining information via cell tower dumps, because such requirements would be unduly restrictive.[251] Cell tower dumps are conducted in the beginning stages of an investigation when law enforcement is trying to establish probable cause; therefore, requiring

---

phone tracks location, responding: "[I]t's a cell phone that's transmitting its location by the action of everybody who has a cell phone." *Id.* at 28-29 (citing Transcript of Hearing at 23, United States v. Capito (D. Ariz. Sept. 14, 2011) (No. 3:10-CR-8050)).

244. *See supra* notes 235-43 and accompanying text.

245. *ECPA Hearing*, *supra* note 155, at 76 (materials submitted by the Hon. Robert C. Scott).

246. *Id.* at 79 (materials submitted by the Hon. Robert C. Scott).

247. *Id.* at 28 (statement of Peter A. Modafferi).

248. *In re* United States, 42 F. Supp. 3d 511, 519-20 (S.D.N.Y. 2014) (holding cell tower dumps were not a Fourth Amendment search because of the Third Party Disclosure Doctrine).

249. Owsley, *supra* note 9, at 16.

250. Crusco, *supra* note 13, at 5.

251. *See In re United States*, 42 F. Supp. 3d at 519-20 (holding that an order under 18 U.S.C. § 2701(d) was all that was needed, which does not require probable cause).

probable cause to conduct a cell tower dump would be impractical.[252] A major reason why cell tower dumps are not considered a search under the Fourth Amendment is that they do not provide such specific locations as to violate a person's reasonable expectation of privacy.[253] Instead, cell tower dumps provide only an approximate location of the cell phone, which, in turn, requires law enforcement to do more investigating to determine the exact location of the cell phone.[254] Therefore, law enforcement should be able to obtain information from cell tower dumps without showing probable cause because cell tower dumps are not a Fourth Amendment search.[255] The U.S. Supreme Court must establish a bright line rule in order to clear up confusion for law enforcement regarding the standard necessary to obtain cell tower dumps.[256] It is important to understand the application of the Third Party Disclosure Doctrine to cell tower dumps.[257] Below, this Part will argue that the Mosaic Theory should not be applied to cell tower dumps.[258]

252. *ECPA Hearing*, *supra* note 155, at 19 (statement of Peter A. Modafferi).

253. *Compare In re* U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 311 (3d Cir. 2010) (arguing that cell tower dumps do not provide precise location data as would be available with GPS tracking), *with* Benjamin Burnham, Comment, *Hitching a Ride: Every Time You Take a Drive, The Government Is Riding with You*, 39 J. MARSHALL L. REV. 1499, 1506 (2006) (explaining how E-ZPass records provide police with much more accurate and precise location data).

254. *Compare In re U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 311 (explaining that cell tower dumps only provide an approximate location, requiring law enforcement to do more work to draw connections), *with* Burnham, *supra* note 253, at 1506 (arguing that "EZ-Pass is basically [] enabling a tracking system" because the location data is so precise).

255. *In re* United States, 42 F. Supp. 3d at 519-20 (holding cell tower dumps were not a Fourth Amendment search).

256. *ECPA Hearing*, *supra* note 155, at 20 (statement of Peter A. Modafferi) (arguing that cell tower dumps provide the building blocks of law enforcement investigations); Langer, *supra* note 120, at 972 (explaining a Supreme Court decision on the issue of cell-site information is a possible solution to the issue); *see infra* Part IV.A; *see also supra* Part III.A–B (illustrating the confusion created by the lack of clarity in the law and in the courts regarding the standard necessary to obtain cell tower dumps); *supra* Part III.C (discussing the problems that requiring probable cause to obtain cell tower dumps would create for law enforcement).

257. *See In re United States*, 42 F. Supp. 3d at 519-20 (holding cell tower dumps were not a Fourth Amendment search because of the Third Party Disclosure Doctrine); *infra* Part IV.B.

258. *See* Evan Bernick, *Protecting American's Privacy: Why the Electronic Communications Privacy Act Should Be Amended*, HERITAGE FOUND. LEGAL MEMORANDUM 1, 6 (2014), http://thf_media.s3.amazonaws.com/2014/pdf/LM118.pdf (arguing that the Mosaic Theory provides more Fourth Amendment protection than the Third Party Disclosure Doctrine does, but that the Mosaic Theory does not provide clear guidelines for law enforcement and the courts); *infra* Part IV.C.

A. A Bright Line Rule Should Be Established to Clear Up Law Enforcement's Confusion Regarding the Standard Necessary to Obtain Cell Tower Dumps

Even though cell tower dumps do not constitute a Fourth Amendment search, the Supreme Court should establish that the specific and articulable facts standard be universally applied to cell tower dumps in the interest of providing some protection.[259] This ensures that law enforcement has some basis as to why the information received after a cell tower dump would be helpful, and protects individuals against law enforcement requesting cell towers dumps for no reason.[260] At the same time, the specific and articulable facts standard would be less restrictive and require a lesser showing than probable cause, making it easier for law enforcement in the initial stages of an investigation to gather the information necessary to establish probable cause.[261] Further, Senator Markey's proposed legislation on cell tower dumps would not require a warrant to conduct cell tower dumps, suggesting that Congress does not believe a warrant supported by probable cause is necessary.[262] All that the proposed legislation would seek to do is restrain law enforcement's access to cell tower dumps by requiring that the requests are more carefully modified, so as to protect those who are not involved in the crime under investigation, but whose cell phones were connected to the tower in question, which can be done by requiring specific and articulable facts.[263]

Requiring probable cause at such an early stage in investigations would make solving crimes unnecessarily difficult.[264] In particular, because cell tower dumps are requested with no suspect in mind, cell tower dumps constitute an invaluable investigatory tool used by law enforcement.[265] During the beginning stages of an investigation, law

---

259. *ECPA Hearing*, *supra* note 155, at 20 (statement of Peter A. Modafferi) (arguing that requiring probable cause for such basic and limited information would make it much more difficult for law enforcement to solve crimes).

260. *Id.* (arguing that there needs to be a balance between the standards to access cell tower dumps and the investigatory benefits for law enforcement in using cell tower dumps).

261. *Id.* at 26 (arguing that "[i]nvestigations don't start with probable cause; they lead to probable cause"); *see also id.* at 16-17 (statement of Mark Eckenwiler) (explaining cell tower dumps have the potential to revel vast amounts of innocent bystander information so some privacy protection should be afforded, even though Mr. Eckenwiler does not suggest how to do this).

262. Nakashima, *supra* note 9, at A1; *see supra* note 216 and accompanying text (explaining the privacy protections a district court judge required the government to include along with the specific and articulable facts to establish why the cell tower dump was necessary).

263. *See supra* note 100 and accompanying text.

264. *ECPA Hearing*, *supra* note 155, at 19 (statement of Peter A. Modafferi); *see supra* Part III.C.

265. *ECPA Hearing*, *supra* note 155, at 19 (statement of Peter A. Modafferi).

enforcement often has little information regarding potential suspects.[266] The use of information attained following a cell tower dump allows law enforcement to "winnow out and prioritize leads from the unorganized mass of related and unrelated information that surrounds a crime and a crime scene."[267]

Additionally, with cell tower dumps, law enforcement is generally not looking into a specific cell phone number or user.[268] Rather, it is looking into the cell phones in a given area, at a given time, on a given date.[269] When law enforcement seeks to use cell tower dumps it is using this technique to help it identify cell phones that are used near a specific location on a certain day at a given time.[270] Essentially law enforcement is starting with nothing and uses the information provided in the cell tower dump as the building block of their investigation.[271] When a cell tower dump is requested, all law enforcement generally obtains is cell phone numbers and basic customer information including names and billing information.[272] However, law enforcement does not get an exact location of a person's cell phone.[273]

In addition to providing law enforcement with important information during the early stages of an investigation, cell tower dumps are not as invasive to a person's privacy as other forms of cell-site location data.[274] Cell tower dumps do not provide an exact location for a cell phone and its user.[275] Instead, cell towers dumps indicate which cell tower was used during cellular communication.[276] Cell tower dumps provide information more beneficial for cell service providers to manage their networks than to provide law enforcement with tracking capabilities.[277] Cell tower data is less precise and less intrusive than other forms of cell phone technology, such as GPS or real-time cell-site location data, making a warrant unnecessary.[278]

---

266. *Id.* at 23.

267. *Id.*

268. Crusco, *supra* note 13, at 5.

269. *Id.*

270. *Id.*

271. *ECPA Hearing*, *supra* note 155, at 19 (statement of Peter A. Modafferi).

272. Nakashima, *supra* note 9, at A1, A8.

273. Owsley, *supra* note 9, at 6.

274. *See supra* note 21 (explaining how real-time cell-site location information essentially allows law enforcement to track a person's cell phone in real time).

275. Owsley, *supra* note 9, at 6.

276. *ECPA Hearing*, *supra* note 155, at 6 (testimony of Mark Eckenwiler).

277. Douglas Starr, *What Your Cell Phone Can't Tell the Police*, NEW YORKER (June 26, 2014), http://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police.

278. Ellen Nakashima, *To Obtain Cellphone Location Records, Warrant Is Needed Says Federal Appeals Court*, WASH. POST (June 11, 2014), http://www.washingtonpost.com/world/national-security/to-obtain-cellphone-location-records-warrant-is-needed-says-federal-

Cell tower data is also less invasive or precise than the data law enforcement officials obtain when they use E-ZPass records in the course of their investigation.[279] When law enforcement officials request E-ZPass records, they are only required get a subpoena, which does not require a showing of probable cause.[280] E-ZPass records are essentially a tracking system, because each time an E-ZPass user travels through a tollbooth, the date, time, and tollbooth location is transmitted to a central computer.[281] This provides law enforcement with an exact historical location of a person, allowing them to track that person's movements.[282] However, cell tower dumps merely provide law enforcement with an approximate location of a person's cell phone.[283] Therefore, it would be illogical to require a warrant supported by probable cause for cell tower dumps, where law enforcement only gets a list of phone numbers, when only a subpoena is required for E-ZPass records, which essentially provides law enforcement with tracking information.[284] E-ZPass, like cell tower dumps, is an innovative technological practice used by those E-ZPass users who have chosen to trade privacy for convenience.[285] Since *Katz* is primarily concerned with privacy, when "people choose to capitalize on the convenience of E-ZPass even though they know it creates a record of their toll crossings, then *Katz* will not protect them."[286] If the Supreme Court were not to allow law enforcement to utilize these new innovations, the Court would essentially "confine law enforcement to primitive means for detecting and investigating evidence of crime."[287]

Cell tower dumps can be used to confirm whether or not that suspect was actually at the scene.[288] Law enforcement can confirm or dismiss alibi statements of the suspect claiming not to be near the scene

---

appeals-court/2014/06/11/a21a73a2-f1ab-11e3-914c-1fbd0614e2d4_story.html; *see also* Crusco, *supra* note 13, at 5 (arguing that courts have determined cell phone pinging does not require a warrant despite the greater accuracy in tracking the cell phone users location).

279. Owsley, *supra* note 9, at 6; Burnham, *supra* note 253, at 1506.

280. Burnham, *supra* note 253, at 1506.

281. *Id.*

282. *Id.*

283. Owsley, *supra* note 9, at 6.

284. Crusco, *supra* note 13, at 5; *see also* Burnham, *supra* note 253, at 1506.

285. Christopher Caldwell, *A Pass on Privacy?*, N.Y. TIMES MAG., July 17, 2005, at 13, 13; *see also* R "Ray" Wang, *Beware Trading Privacy for Convenience*, HARV. BUS. REV. (June 10, 2013), https://hbr.org/2013/06/beware-trading-privacy-for-con.

286. Erin Murphy, Term Paper, *Back to The Future: The Curious Case of* United States v. Jones, 10 OHIO ST. CRIM. L. 325, 335 (2012).

287. Burnham, *supra* note 253, at 1512.

288. *ECPA Hearing*, *supra* note 155, at 23 (statement of Peter A. Modafferi).

of the crime at the time the crime was committed.[289] Further, law enforcement can confirm witness statements that a particular person was involved in the crime by cross checking the information received via a cell tower dump.[290] The use of cell tower dumps can protect potential suspects from wrongful arrests because cell tower dumps provide a more accurate picture of who was in the vicinity of a crime scene at the time the crime was committed.[291] Wrongful arrests often result when police are unable to conduct adequate investigations, but allowing cell tower dumps to be used without requiring probable cause will allow law enforcement to conduct more complete investigations.[292] In particular, cell tower dumps provide law enforcement with crucial information at the critical early stages of an investigation where mistakes are more likely to occur.[293] The information obtained via cell tower dumps is an essential element of helping law enforcement establish probable cause.[294] Therefore, it would be unduly restrictive to require a showing of probable cause before the information could even be obtained.[295]

B. The Third Party Disclosure Doctrine Applies to Cell Tower Dumps, Making Them a Search Exception to the Fourth Amendment

Cell tower dumps cannot violate a person's reasonable expectation of privacy because individuals voluntarily disclose their cell phone information to cell service providers, thus falling outside the protected zone of privacy.[296] Cell tower dumps should not constitute a Fourth Amendment search because they are a form of business records

289. *Id.* (discussing the utility of cell tower dump data to confirm or dismiss an alibi statement by seeing if the suspects phone was at the crime scene).

290. *Id.* (illustrating the utility of cell tower dump data to confirm or dismiss witness statements that they were at the crime scene).

291. *Id.* at 19 (arguing that mistaken identifications are the primary cause of wrongful convictions and using cell tower dump data can help prevent this by confirming the suspect was actually at the crime scene).

292. *Id.* at 24. Preventing wrongful convictions begins at the crime scene because there "cannot be a wrongful conviction without a wrongful arrest." *Id.* Wrongful arrests result when law enforcement believes it has solid evidence but that proof is not concrete. *Id.*

293. *Id.* (arguing cell tower data is "tremendous[ly] factual data that can be used to remedy these failures").

294. *Id.* at 24, 26.

295. *Id.*

296. *See In re* United States, 42 F. Supp. 3d 511, 519-20 (S.D.N.Y. 2014) (applying the Third Party Disclosure Doctrine, the court determined cell tower dumps are not a Fourth Amendment search); Hamblett, *supra* note 217, at 6.

voluntarily conveyed to a third party.[297] E-ZPass technology, like cell phone technology, has been heralded as an innovation where the user trades some privacy for convenience.[298] Some would argue that the unrestrained access to this information would be contrary to the core values of the Fourth Amendment.[299] However, E-ZPass records, like cell tower dumps, are business records and are, therefore, exempt from Fourth Amendment restrictions.[300] Because E-ZPass users elect to use the system as a way of making travel faster, they are voluntarily conveying their location information to E-ZPass.[301] This is the same as when cell phone users make a phone call, connecting to a cell tower, as they are voluntarily conveying this information to the cell service provider.[302] Therefore, the Third Party Disclosure Doctrine protects both E-ZPass records and cell tower dumps from Fourth Amendment restrictions.[303]

Further, the Obama Administration argued that Americans do not enjoy a reasonable expectation of privacy in their location while using a cell phone, citing the Third Party Disclosure Doctrine as the authority for this assertion.[304] Additionally, lower courts held that, under the existing law, a cell phone user lacks a reasonable expectation of privacy in information obtained via cell tower dumps.[305] Based on clear Supreme Court precedent, lower courts have determined the Third Party Disclosure Doctrine is applicable to cell tower historical cell-site location data—of which cell tower dumps are a subset—because "[a]s part of the ordinary course of business, cellular phone companies collect information that identifies the cell towers through which a person's calls are routed."[306]

Since the customer gives the information obtained through the use of cell tower dumps to the phone company, the information is not

297. *See* Smith v. Maryland, 442 U.S. 735, 744-46 (1979) (holding the Third Party Disclosure Doctrine extended to telephone numbers dialed); United States v. Miller, 425 U.S. 435, 443 (1976) (holding information voluntarily conveyed to a third party was beyond the scope of Fourth Amendment protections).

298. Caldwell, *supra* note 285, at 13; *see* Wang, *supra* note 285.

299. Murphy, *supra* note 286, at 326.

300. *In re United States*, 42 F. Supp. 3d at 519; *ECPA Hearing*, *supra* note 155, at 19 (statement of Peter A. Modafferi); *see* Murphy, *supra* note 286, at 335.

301. Burnham, *supra* note 253, at 1506; Murphy, *supra* note 286, at 335.

302. *In re* United States, 42 F. Supp. 3d at 517-18.

303. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

304. Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010, 4:00 AM), http://web.archive.org/web/20140209075310/http://news.cnet.com/8301-13578_3-10451518-38.html.

305. *In re* Smartphone Geolocation Data Ass'n, 979 F. Supp. 2d 129, 147 (E.D.N.Y. 2013).

306. United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012).

afforded Fourth Amendment protections.[307] Customers are voluntarily disclosing information regarding their cell phone data to cell service providers by signing a contract with them for their services, thus risking that the cell service providers will disclose the information to the government without their express knowledge or approval.[308] While Justice Sotomayor's consenting opinion in *Jones* suggests the era of the applicability of the Third Party Disclosure Doctrine has passed, until this view is endorsed by the majority of the Supreme Court, the Third Party Disclosure Doctrine is still good law.[309] Moreover, the information obtained via cell tower dumps involves cell phone information "communicated for the purpose of making and receiving calls in the ordinary course of the provision of cellular phone service."[310] Cell phone users understand that when they are outside the network of their service provider, their cell phone does not work.[311] Therefore, cell phone users know that when they make or receive calls, their cell phones transmit signals to the nearest cell tower, and as a result, to their communications service providers.[312] One court compared cell phone use to providing a telephone operator with the phone number you want dialed because once a person tells the operator the phone number they want dialed, the phone number is no longer confidential.[313] Analogous to *Smith v. Maryland*,[314] a person does not have a reasonable expectation of privacy in the telephone numbers dialed on a home phone, and therefore, it follows that a person does not have a reasonable expectation of privacy in the numbers dialed on a cell phone.[315]

---

307. Nakashima, *supra* note 9, at A9.

308. *See Smith*, 442 U.S. at 744 (extending Third Party Disclosure Doctrine to telephone numbers dialed); *Miller*, 425 U.S. at 443 (establishing the Third Party Disclosure Doctrine).

309. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also* Orin Kerr, *Third Circuit on the Mosaic Theory and* Smith v. Maryland, VOLOKH CONSPIRACY (Sept. 30, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/30/third-circuit-on-the-mosaic-theory-and-smith-v-maryland.

310. United States v. Caraballo, 962 F. Supp. 2d 341, 359-60 (D. Vt. 2013).

311. *In re* Smartphone Geolocation Data Ass'n, 979 F. Supp. 2d 129, 146 (E.D.N.Y. 2013); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012).

312. *In re Smartphone Geolocation Data Ass'n*, 979 F. Supp. 2d at 146; *see Madison*, 2012 WL 3095357, at *8.

313. United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012); Crusco, *supra* note 13, at 8.

314. 442 U.S. 735 (1979); *see supra* notes 121-26 and accompanying text (discussing the details of the *Smith v. Maryland* case).

315. *Smith*, 442 U.S. at 744-45; *see also* Orin Kerr, *Third Circuit Rules that Magistrate Judges Have Discretion to Reject non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records*, VOLOKH CONSPIRACY (Sept. 8, 2010, 2:23 PM), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records (explaining how the pen registers used in *Smith* provided an exact location, yet the Court found the location where the call originated was immaterial, whereas in cell tower dump cases, the location of

C. *The Mosaic Theory Should Not be Applied to Cell Tower Dumps*

Cell tower dumps should not be subject to the Mosaic Theory because they provide very limited information about a person.[316] The Mosaic Theory posits that a collection of technological surveillance data from a variety of sources paints a vivid and deeply personal portrait of an individual.[317] While the Mosaic Theory can offer greater protection than the Third Party Disclosure Doctrine, "it does not offer courts or law enforcement authorities an objective means by which to distinguish conduct that amounts to a search from conduct that does not."[318]

While each individual piece of technological surveillance data does not constitute a Fourth Amendment search, when combined and looked at in its totality, it is evident that an individual's reasonable expectation of privacy is violated.[319] Thus, the totality of the evidence is a Fourth Amendment search.[320] Since only minimal constitutional protection is applied when location data facilitates the discovery of information that already enjoys constitutional protection, the location data becomes part of the mosaic.[321] Cell tower dumps are not afforded constitutional protection because they do not constitute a search protected by the Fourth Amendment; thus, they are not part of the

---

where the call originated appears to be the entire crux of the issue).

316. *Compare* United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010) (applying the Mosaic Theory to GPS tracking because it provides an intimate portrait of an individual's life), *with In re* United States, 42 F. Supp. 3d 511, 515-16 (S.D.N.Y. 2014) (finding that cell tower dumps do not allow for the possibility of widespread tracking). Since GPS tracking provides a more vivid picture of a person's life than cell tower dumps, the Mosaic Theory is applicable to GPS tracking and not to cell tower dumps. *In re United States*, 42 F. Supp. 3d, at 515-16; *Maynard*, 615 F.3d. at 561-62.

317. *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (applying the Mosaic Theory to GPS tracking and stating that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familiar, political, professional, religious, and sexual associations").

318. Bernick, *supra* note 258, at 5-6 (arguing the Third Party Disclosure Doctrine provides clarity for law enforcement and courts).

319. Ken Strutin, *Mosaic Theory: A New Perspective for Human Privacy*, 250 N.Y. L.J. 5, 7 (2013).

320. Kerr, *supra* note 150, at 320. Under this approach:

> The mosaic theory requires the courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group.

Id.

321. Bellovin et al., *supra* note 106, at 583.

mosaic.[322] The Mosaic Theory has also been described as "[d]isparate items of information [that], though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information."[323]

However, this is not applicable to the information obtained via cell tower dumps because that information is extremely limited.[324] Justice Sotomayor suggested that the Mosaic Theory should be applied when the government learns details about a person's personal life "more or less at will."[325] However, cell tower dumps only provide a list of phone numbers, not the record of a person's precise movements and intimate reflection of an individual's personal life that is created by GPS data.[326] Cell tower dumps only provide a list of phone numbers that were in the vicinity of the cell tower on the date and time in question.[327] Not only is this very limited information, but it is also extremely valuable to law enforcement.[328] Cell tower dumps also differ from the more typical cases where the Mosaic Theory is applied, such as GPS tracking cases, because law enforcement is not getting exact and precise information.[329]

In *United States v. Maynard*,[330] the Majority argued that prolonged surveillance reveals greater detail about a person's private life.[331] However, when law enforcement utilizes cell tower dumps, it is only requesting periods of time up to two hours.[332] Justice Sotomayor argued in her concurring opinion in *Jones* that the Mosaic Theory becomes applicable in the digital age because, with advances in technology, law enforcement has greater access to an entire picture of a person's life without restriction.[333] While that may be true for forms of technology like GPS tracking, that is not the case for cell tower dumps because of

322. *See supra* Part IV.A–B.

323. David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005); Kerr, *supra* note 150, at 320.

324. Crusco, *supra* note 13, at 5.

325. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

326. Crusco, *supra* note 13, at 5.

327. *Id.*

328. *See supra* Part IV.A.

329. *See Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010); People v. Weaver, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009).

330. 615 F.3d 544 (D.C. Cir. 2010).

331. *Maynard*, 615 F.3d. at 562; Kerr, *supra* note 150, at 326.

332. Nakashima, *supra* note 9.

333. *Jones*, 132 S. Ct.at 955 (2012) (Sotomayor, J., concurring).

the limited information law enforcement actually obtains.[334] Justice Alito suggested that the Mosaic Theory is applicable when law enforcement gathers and analyzes evidence in a way that would surprise members of society.[335] It is not a surprise to any member in today's society that cell service providers collect the outgoing and incoming call information of cell phone users, because people today understand that this is the ordinary course of business for cell service providers.[336] Further, when law enforcement uses GPS tracking, or even real-time cell-site location data, it has a particular target.[337] But, it does not have a particular person or cell phone number that it is targeting when it does a cell tower dump; rather, law enforcement uses cell tower dumps at the early stages of an investigation to find suspects and get the necessary information to establish probable cause.[338] Thus, using all the available investigative tools to create the portrait of a person or situation is good investigative work by law enforcement, not a search in violation of the Fourth Amendment.[339]

V. CONCLUSION

Cell tower dumps do not constitute a search under the Fourth Amendment because they do not violate a person's reasonable expectation of privacy.[340] They reveal such a limited amount of information about an individual that they should not be subject to the higher standard of probable cause; rather, the specific and articulable facts standard is sufficient.[341] When law enforcement uses cell tower dumps, it is not singling out a specific phone number that they want information about.[342] Instead, law enforcement is looking at records of

334. Crusco, *supra* note 13, at 5 (explaining that all law enforcement really gets from cell tower dumps is a list of outgoing and incoming phone calls to that particular cell tower).

335. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *ECPA Hearing*, *supra* note 155, at 105 (statement of Mark Eckenweiler); Kerr, *supra* note 150, at 330.

336. *See supra* Part IV.B.

337. *See Jones*, 132 S. Ct. at 948 (explaining that police targeted Jones because he was suspected of being a drug dealer); *supra* note 21.

338. *ECPA Hearing*, *supra* note 155, at 24 (statement of Peter A. Modafferi); Crusco, *supra* note 13, at 5.

339. *ECPA Hearing*, *supra* note 155, at 26-27 (statement of Peter A. Modafferi).

340. *See supra* Part IV.B.

341. *See supra* Part III.B–C.

342. Crusco, *supra* note 13, at 5.

all incoming and outgoing phone calls that were bounced off a particular cell tower on a given date and time.[343] Since cell phone users voluntarily disclose their location information to cell service providers, they assume the risk that their cell service provider will convey this information to a third party.[344] The information obtained from cell tower dumps are the business records of the cell service providers kept in the ordinary course of business.[345] This is understood by cell phone users because there is widespread public knowledge of ability and practice of cell phone service providers to track customers' locations.[346] Finally, the Mosaic Theory is not applicable because the information obtained via cell tower dumps does not create a vivid portrait about an individual's personal life—all cell tower dumps provide is a list of incoming and outgoing calls that were facilitated by a specific cell tower.[347] This does very little to provide law enforcement with more than a picture of the cell phone users in the vicinity of the cell tower, and it certainly does not give a vivid portrait of one particular cell phone user on that list.[348]

Essentially, cell tower dumps only provide law enforcement with a list of cell phone numbers that were being used at a particular time, on a particular date, in a given location.[349] From there, law enforcement must do additional work to track down leads to establish probable cause.[350] The information obtained from cell tower dumps is a crucial building block of investigations, and to require a showing of a higher standard to obtain such information would severely hinder the efficiency of law enforcement and could even have deadly consequences in solving crimes.[351] The Supreme Court needs to establish a bright line rule providing that in order for the government to obtain information via cell tower dumps, it must show specific and articulable facts.[352] This would

343. *See supra* Part IV.A.

344. United States v. Miller, 425 U.S. 435, 443 (1976); *see supra* notes 298-303 and accompanying text (comparing cell tower dumps and E-ZPass records).

345. United States v. Caraballo, 962 F. Supp. 2d 341, 259-60 (D. Vt. 2013).

346. *In re* Smartphone Geolocation Data Association, 979 F. Supp. 2d 129, 146-47 (E.D.N.Y. 2013).

347. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); Crusco, *supra* note 13, at 5.

348. Crusco, *supra* note 13, at 5.

349. *Id.*

350. *ECPA Hearing*, *supra* note 155, at 26 (statement of Peter A. Modafferi).

351. *Id.* at 28 (statement of Peter A. Modafferi).

352. *See supra* Part IV.A.

protect the privacy interests of individuals, while still allowing law enforcement to use all the investigatory tools at their disposal to efficiently and effectively carry out their investigations.[353]

*Amanda Regan**

353. *See supra* Part IV.A.

* J.D. candidate 2016, Maurice A. Deane School of Law at Hofstra University; B.A. in Political Science 2013, Washington College. This Note is dedicated to my family and friends who have all provided me with unending love and support. To my parents, Kevin and Diane Regan, thank you for teaching me the value of hard work, for always believing in me and for supporting my dreams. To my sister, Christina Regan, you inspire me every day; keep pursuing your dreams because you have the talent and determination to make them happen. A special thank you to Professor Fred Klein who has been a wonderful teacher and mentor. I am eternally grateful to everyone on *Hofstra Law Review*, and especially to Aaron Zucker, Addie Katz, Courtney Klapper, Peter Guinanne, Leron Solomon, Michael Senders, Rachel Summer, Nicole Della Ragione, Chibogu Nneka Nzekwu, and the rest of the Volume 44 Board. I would also like to thank the staff of Volume 43 for all their assistance in publishing this Note.

***