University of Richmond Law Review

Volume 51
Issue 3 *National Security in the Information Age: Are We Heading Toward Big Brother? Symposium Issue 2017*

Article 7

3-1-2017

Digital Technology and Analog Law: Cellular Location Data, The Third-Party Doctrine, and the Law's Need to Evolve

Justin Hill
University of Richmond School of Law

DIGITAL TECHNOLOGY AND ANALOG LAW: CELLULAR LOCATION DATA, THE THIRD-PARTY DOCTRINE, AND THE LAW'S NEED TO EVOLVE

INTRODUCTION

Law enforcement agencies consistently utilize Cell Site Location Information ("CSLI") generated by a suspect's cell phone to place that suspect at the scene of a crime. Despite the widespread use of these tactics, consensus in the legal realm regarding the Fourth Amendment's protection of CSLI remains unrefined. The most recent federal circuit courts to address the issue have each applied the third-party doctrine to find no Fourth Amendment protection of the CSLI information in question.[1] However, this apparent uniformity is deceptive. Two of those circuits came to opposite conclusions before the panel opinions were reversed en banc.[2] Each decision has also been met with vociferous opposition within the circuit.[3] Furthermore, the Third Circuit, the first to address the issue, found that the third-party doctrine did not apply at all.[4] Adding fuel to the fire, three state high courts have taken on the issue and found the gathering of at least some forms of CSLI without a search warrant unconstitutional on state

1. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 889–90 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 512–13 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479, 479–80 (2015); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013).

2. United States v. Graham, 796 F.3d 332, 361 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421, 424 (4th Cir. 2015); United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498, 513 (11th Cir. 2015).

3. *See Carpenter*, 819 F.3d at 893–94 (Stranch, J., concurring) (expressing concern over the Fourth Amendment implications of the CSLI collection but stopping short of a Fourth Amendment analysis because the good-faith exception would apply); *Graham*, 824 F.3d at 441–42 (Wynn, J., dissenting in part and concurring in judgment); *Davis*, 785 F.3d at 533 (Martin, J., dissenting); *In re* United States for Historical Cell Site Data, 724 F.3d at 615–16 (Dennis, J., dissenting).

4. *In re* United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317–18 (3rd Cir. 2010) (noting that a cell phone customer does not voluntarily share his location information with a cellular provider in any meaningful way, which would in turn defeat any application of the third-party doctrine).

grounds.[5] Twelve additional states have statutorily insured privacy protection in at least some forms of CSLI data.[6]

Courts have been grappling with this issue at a unique moment for constitutional law. The Supreme Court, while not directly examining CSLI or the third-party doctrine, has re-examined Fourth Amendment doctrine as it comes into conflict with the digital age. In 2012, the Supreme Court addressed the problem of long-term Global Positioning System ("GPS") monitoring under the Fourth Amendment.[7] Justice Sotomayor remarked in her concurrence that the third-party doctrine "is ill suited to the digital age."[8] In 2014, the Court examined the search incident to arrest doctrine in the modern digital age and held that it does not extend to searching the contents of a cell phone.[9] These cases demonstrate that the Supreme Court is prepared to adjust decades-old doctrine in light of technologic advances.

This comment explores how broader shifts in Fourth Amendment doctrine may affect the government's collection of CSLI moving forward. It consists of three parts. Part I examines the technological underpinnings of cellular networks. The issue is frequently litigated, but few in the legal community have a real grasp on the technology. A nuanced understanding of the technology is crucial when examining the accuracy of CSLI or how the third-party doctrine ought to apply. This comment consolidates and simplifies the technical workings of cellular networks to enable better and more informed answers. Last, drawing on this understanding, Part I explores the generation, relative accuracy, and collection of CSLI.

---

5. *See* Tracey v. Florida, 152 So.3d 504, 526 (Fla. 2014) (holding that the collection of active CSLI, absent a warrant, is unconstitutional); Commonwealth v. Augustine, 4 N.E.3d 846, 849–50 (Mass. 2014) (holding that the collection of historical CSLI is unconstitutional without a showing of probable cause); New Jersey v. Earls, 70 A.3d 630, 644 (N.J. 2013) (holding warrantless collection of active CSLI to be unconstitutional on state grounds).

6. *See* COLO. REV. STAT. § 16-3-303.5(2) (2015); 725 ILL. COMP. STAT. 168/10 (2012); IND. CODE § 35-33-5-12(a) (2016); ME. STAT. tit. 16, § 648 (2016); MD. CODE ANN., CRIM. PROC. § 1-203.1(b)(1) (LexisNexis 2013); MINN. STAT. §§ 626A.28(3)(d), 626A.42(2)(a) (2016); MONT. CODE ANN. § 46-5-110(1)(a) (2015); TENN. CODE ANN. § 39-13- 610(b) (2016); UTAH CODE ANN. § 77-23c-102(1)(a) (LexisNexis 2015); VA. CODE ANN. § 19.2-56.2(B) (2015); WASH. REV. CODE § 9.73.260(2) (2015); WIS. STAT. § 968.373(2) (2016).

7. United States v. Jones, 565 U.S. 400, 402 (2012).

8. *Id.* at 417 (Sotomayor, J., concurring).

9. Riley v. California, 134 S. Ct. 2473, 2484–85 (2014).

Part II examines the law with regards to CSLI. It begins with the statute governing CSLI collection and then assesses the Supreme Court precedent relevant to CSLI litigation: namely the third-party doctrine and cases dealing with physical location tracking. Part II will also examine *United States v. Jones*,[10] *Riley v. California*,[11] and their potential impact on the field. Last, it consolidates the five circuit court opinions to address CSLI.

Part III utilizes a more nuanced understanding of cell phone technology in applying the third-party doctrine. In doing so, two propositions become immediately evident. First, the superficial understanding of cell phone technology has led to inaccurate decisions on both sides of the CSLI debate. In particular, there is a critical, yet overlooked, distinction between user-generated and non-user-generated CSLI information due to the way that CSLI information is created in cellular networks.

Second, it becomes clear that the current state of the law is, as Justice Sotomayor recently put it, "ill suited for the digital age."[12] A proper application of the third-party doctrine presents two distinct problems. First, it places courts in the untenable position of becoming subject matter experts on complex technology in order to decide constitutional questions. In the realm of Fourth Amendment doctrine, courts need to establish bright-line rules that law enforcement can apply, not overly nuanced decisions based on the specific operations of different technologies.

Second, a proper application of the third-party doctrine allows law enforcement to glean CSLI information that would be both under- and overinclusive of their needs. They would be able to collect user-generated CSLI from time frames extending long before and after a crime. However, law enforcement would be unable to collect non-user-generated CSLI through a court order, even for the exact time a crime was committed.

These results flow directly from the Fourth Amendment's third-party doctrine yet fail to capture the needs of Fourth Amendment jurisprudence. Congress remains either unwilling or incapable of modifying existing law to protect basic privacy concerns and ensure law enforcement needs. Therefore, the CSLI de-

10. 565 U.S. 400 (2012).
11. 134 S. Ct. 2473 (2014).
12. 565 U.S. at 417 (Sotomayor, J., concurring).

bate is now ripe for certiorari and the Supreme Court should rule on an area of law that has become unclear and outdated.

I. THE TECHNOLOGY BEHIND CELLULAR COMMUNICATION AND CSLI DATA

A. *The Fundamentals of Wireless Communication*

Cell phones communicate through radio waves.[13] Radio waves are a type of electromagnetic wave and move at the speed of light.[14] Electromagnetic waves come in a wide variety of types and are classified according to their frequency.[15] Starting from the smallest frequency, electromagnetic waves are classified as either gamma rays, x-rays, ultraviolet light, visible light, infrared light, microwaves, or radio waves.[16]

Through a process called modulation, radio waves can be used to carry information.[17] In modulation, a single known frequency is used as a carrier wave.[18] The modulation process modifies the carrier wave to superimpose information on it.[19] After this wave is sent, the receiving device reverses the process, demodulating the wave to receive the transmitted information.[20] This process of modulation is the basic premise behind all wireless technology.[21] However, as anybody who has ever used a two-way radio has undoubtedly realized, a handset can only broadcast a signal a certain distance. This is where cellular networks become important.

---

13. *See* IAN POOLE, CELLULAR COMMUNICATIONS EXPLAINED: FROM BASICS TO 3G 13 (2006), http://dinus.ac.id/repository/docs/ajar/Cellular_Communications.pdf.

14. *See Anatomy of an Electromagnetic Wave*, NAT'L AERONAUTICS & SPACE ADMIN. (2010), http://missionscience.nasa.gov/ems/02_anatomy.html.

15. *See* POOLE, *supra* note 13, at 18. Electromagnetic waves can alternatively be classified by wavelength as well because wavelength and frequency have a direct inverse relationship. *See id.* at 17. Electromagnetic waves moving through a vacuum have a frequency of the speed of light divided by their wavelength or, alternatively, their wavelength is the speed of light divided by their frequency. *Id.*

16. *The Electromagnetic Spectrum*, NAT'L AERONAUTICS & SPACE ADMIN. (2013), http://imagine.gsfc.nasa.gov/science/toolbox/emspectruml.html.

17. POOLE, *supra* note 13, at 27.

18. *Id.*

19. *Id.* Morse code is the simplest example of amplitude modulation. *Id.* With Morse code, the carrier wave's amplitude is altered to the point of the on or off. *Id.* More sophisticated modulation techniques alter the carrier wave in order to represent binary information. *See, e.g.*, *id.* at 38 (discussing phase reversal keying).

20. *Id.* at 27.

21. *See Modulation*, TECHOPEDIA, http://www.techopedia.com/definition8409/modulaton (last visited Feb. 13, 2017).

B. *The Fundamentals of Cellular Networks*

Cellular networks give a person the ability to speak to another person over significant distances. Cellular networks act as a middle man, carrying the signal from the transmitter to its recipient. All cellular networks consist of three overarching sections.[22] First, and most recognizable, each network has what is commonly called the radio network.[23] The radio network consists of all the cell towers, antennas, and other equipment that is necessary to provide network connectivity.[24] The second section of every network is commonly known as the core network.[25] The core network consists of everything that is necessary for the proper switching and routing of calls, as well as subscriber management.[26] The last section is the intelligent network.[27] The intelligent network provides additional network functionalities, such as managing prepaid services and other billing actions.[28]

1. The Cellular Network

There are two predominate types of cellular networks in the United States: the Global System for Mobile Communications ("GSM") networks and the Code Division Multiple Access ("CDMA") networks.[29] GSM is utilized by AT&T and T-Mobile, amongst others.[30] CDMA networks include those operated by Verizon Wireless, Sprint, and U.S. Cellular.[31] Originally, the two protocols differed significantly in how the radio wave spectrum was divided and utilized.[32] However, following the upgrade to third-

22. POOLE, *supra* note 13, at 156. Different cellular standards and providers utilize different techniques and terminology. *Id.* at 60. However, all networks can be put into general categories based on having the same requisite technological needs.

23. *Id.* at 156; MARTIN SAUTER, FROM GSM TO LTE-ADVANCED: AN INTRODUCTION TO MOBILE NETWORKS AND MOBILE BROADBAND 11 (2d ed. 2014). Radio network is a general term. Some subsystems term this section the radio access network ("RAN"), while others call it the base station subsystem ("BSS"). *See id.*; POOLE, *supra* note 13, at 158.

24. SAUTER, *supra* note 23, at 11–12.

25. *Id.* at 12. The core network is also known as the Network Subsystem ("NSS"). *Id.*

26. *Id.*

27. *Id.* More formally, this is called the Intelligent Network Subsystem ("IN"). *Id.*

28. *Id.*

29. Sascha Segan, *CDMA vs. GSM: What's the Difference?*, PC MAG. (Feb. 6, 2015, 10:03 AM), http://www.pcmag.com/article2/0,2817,2407896,00.asp.

30. *Id.*

31. *Id.*

32. The methods which divide and utilize the radio wave spectrum are called multiple access schemes. POOLE, *supra* note 13, at 53. GSM originally utilized a combination of

generation (3G) technology in the early 2000s, both protocols began utilizing similar CDMA-based technology.[33] This trend towards consolidation has continued as both groups of network providers have begun implementing fourth-generation Long-Term Evolution ("4G LTE") and LTE Advanced protocols.[34]

Due to the use of older cell phones, networks must remain backwards compatible. Thus, network providers still incorporate some aspects of older GSM or CDMA protocols.[35] Accordingly, networks are still typically labeled as either GSM or CDMA, even though the distinction is quickly evaporating.[36] Overall, GSM and CDMA networks are remarkably similar. Both contain the same three basic subsections: the radio network, core network, and intelligent network.[37] Furthermore, both types of networks are structured similarly. For simplicity, this comment will explain cellular fundamentals in general, as is applicable to all types of networks. However, pertinent terminology distinctions are noted throughout.

Frequency Division Multiple Access ("FDMA") and Time Division Multiple Access ("TDMA"). *Id.* at 53–54. This meant that each tower on the network utilized a different range of frequencies. *See id.* at 84. Then the tower would assign small sections of that frequency range to each phone it was connected to. *See id.* at 54. Each of those frequency ranges were then subdivided into discrete time slots. *See id.* This enabled one discrete frequency to be utilized by multiple cell phones, who would take turns sending short bursts of data during assigned time slots. *See id.* CDMA, as the name suggests, utilizes codes rather than frequencies to distribute the radio wave spectrum. *Id.* at 114. Each cell phone utilizes unique codes that are used when transmitting information. *See id.* at 115–16. CDMA also uses 64 discrete time slots, each of which are earmarked for specific types of network activity. *Id.* at 114. In this way, the tower receives only one set of data when it listens for a unique code, and vice versa. This is akin to a roomful of people all speaking different languages. *Id.* at 55. Even though the noise level in the room would be very high, a person would still be able to understand somebody speaking their language. *Id.*

33. GSM providers implemented an upgraded protocol called Universal Mobile Telecommunications System ("UMTS") which shifted from an FDMA access method to one based on Wideband CDMA ("W-CDMA"). *Id.* at 155. Around the same time, CDMA networks implemented an updated protocol named CDMA2000. *Id.* at 135. This was a more optimized version of prior CDMA protocols.

34. *See* SAUTER *supra* note 23, at 235. 4G LTE and LTE Advanced both remain CDMA-based protocols. *See id.*

35. *See id.* at 2–3, 201–02 (describing evolution of cellular networks and how newer networks are able to switch back to older forms such as GSM or CDMA because of their structure).

36. *See* POOLE, *supra* note 13, at 79–80.

37. *See* SAUTER, *supra* note 23, at 10, 201 (identifying the networks in GSM as the radio network, core network, and the intelligent network); *see also* POOLE, *supra* note 13, at 156 (explaining how UMTS, a CDMA system, has three subsystems similar to GSM).

a. The Radio Network

The radio network consists of the cell towers, antennas, and other equipment that is necessary to provide network connectivity.[38] Most recognizable amongst these features is a cell tower. The large metal towers supporting cellular network technology have become ubiquitous in the modern landscape. These are not the only cell towers, however. Cell towers come in four major types: macrocells, microcells, picocells, and femto cells.[39] Macrocells and microcells are the towers that most people picture in their minds: large metal structures with antennas at the top. Macrocells provide network coverage for areas about 10 kilometers or greater in diameter around the tower.[40] Microcells provide smaller coverage areas of approximately 200 meters to 2 kilometers in diameter.[41] Picocells serve much smaller areas—approximately 4 to 200 meters.[42] They are often utilized to cover areas such as tunnels or particular sections of buildings.[43] Femto cells are the smallest, with a typical cell size of 10 meters.[44] In the end, regardless of its type, the tower is known as a Base Transceiver Station ("BTS").[45] Commonly, BTSs are simply referred to as base stations.[46]

Base stations typically provide circular coverage, utilizing multiple antennas. Most commonly, a base station will have three antennas, each covering a 120-degree sector.[47] These individual antennas are known as cells.[48] Cells can only handle connections with a certain number of phones—a concept referred to as capaci-

38. *See* SAUTER, *supra* note 23, at 10; *see also* POOLE, *supra* note 13, at 60–61.

39. POOLE, *supra* note 13, at 53; Dimitris Mavrakis, *Do We Really Need Femto Cells?*, VISION MOBILE (Dec. 1, 2007), https://www.visionmobile.com/blog/2007/12/do-we-really-need-femto-cells.

40. POOLE, *supra* note 13, at 53. Other figures put macrocell size at 1 to 30 kilometers. Mavrakis, *supra* note 39.

41. Mavrakis, *supra* note 39; *see also* POOLE, *supra* note 13, at 53 (explaining that microcells cover areas with a diameter of approximately 1 kilometer).

42. Mavrakis, *supra* note 39.

43. POOLE, *supra* note 13, at 53.

44. Mavrakis, *supra* note 39.

45. SAUTER, *supra* note 23, at 23.

46. *Id.*

47. POOLE, *supra* note 13, at 174. However, base stations will occasionally have more or less antennae. In these events, the overall coverage would still equal 360 degrees. Thus, in a base station with four antennas, each would most likely cover 90 degree sectors. Likewise, two antennas would equate to two 180 degree sectors. *See* SAUTER, *supra* note 23, at 149.

48. *See* POOLE, *supra* note 13, at 52; SAUTER, *supra* note 23, at 23–24.

ty.[49] Any additional phones beyond network capacity would be unable to establish a connection to the network.

Cellular networks are structured to prevent inefficient overlapping coverage, yet ensure sufficient network capacity.[50] The easiest way to understand the basic format this typically takes is to visualize a beehive pattern. In this pattern, each hexagon would typically contain a macro or microcell at the center.[51] From that basic framework the network provider adds towers as network capacity requires.[52] Thus, a largely unpopulated 10 kilometer stretch of land may only have one macrocell serving it. On the other hand, more densely populated areas would require the network to provide a higher capacity. Networks achieve a higher capacity by placing many smaller base stations within this coverage area.[53] For example, a densely populated city might place microcells throughout the city in regular intervals. These towers would then be interspersed with picocells, which could provide more capacity in smaller, high traffic areas. Last, a network provider might further supplement the network by adding femto cells in very small areas that receive extremely high volumes of traffic—such as subway platforms.

The radio network also contains Base Station Controllers ("BSC").[54] BSCs control the base stations and essentially act as their brains.[55] BSCs control all of the actions that occur within the radio network to ensure connectivity and access.[56] One function of particular importance in setting up the basic network is called a handoff.

---

49. *See* SAUTER, *supra* note 23, at 24–25 (describing the channel system and calculations that allow cells to manage their capacity to handle multiple subscribers at the same time); *see also* POOLE, *supra* note 13, at 59–60 (explaining the connection between channels and capacity that allows more users to connect in the network).

50. *See* POOLE, *supra* note 13, at 52.

51. *See id.* at 52–53; SAUTER, *supra* note 23, at 23–24.

52. POOLE, *supra* note 13, at 52.

53. *See* Mavrakis, *supra* note 39 (noting that the most effective way to increase network capacity is to shrink the cell size, which is accomplished by adding more base stations to the existing network).

54. SAUTER, *supra* note 23, at 36.

55. *See id.* In older networks, a single BSC typically controlled a small group of BTSs. However more advanced protocols, such as 4G LTE and LTE Advanced, have begun introducing a new base station called eNode-B. *See id.* at 240–41. These are essentially smart-BTSs, which are capable of individually handling everything that a BSC would have done. *See id.*

56. *See id.* ("[T]he BSC is responsible for the establishment, release and maintenance of all connections of cells that are connected to it.").

Handoffs are the process of switching a cell phone from the cell that is currently providing service to a new one.[57] During calls, the serving cell constantly monitors the signal strength of the transmitting cell phone.[58] If the signal becomes too weak, the base station notifies the network through the BSC.[59] The network will identify a new cell that would provide a stronger connection.[60] Then, the network coordinates the handoff between the cell phone, the current serving cell, and the prospective cell, to ensure a smooth transition.[61] Although easy in concept, the logistics are challenging, as the handoff requires the phone to instantly switch to a new tower's frequency or code without any loss in data.[62] Many can undoubtedly remember the days when calls would seemingly always be dropped while driving. These were the results of unsuccessful handoffs.

b. The Core Network

Every BSC connects to a regional controller known as a Mobile Switching Center ("MSC").[63] The MSC provides connectivity to all of the other databases and outside connections in the core network.[64] Most pertinently, these include the Authentication Center ("AuC"), Equipment Identity Register ("EIR"), Home Location Register ("HLR"), Visitor Location Register ("VLR"), and access to the Public Switched Telephone Network ("PSTN").[65]

The AuC and the EIR serve the network function of ensuring that a particular subscriber and his or her physical cell phone is authorized to access the network. The AuC stores and validates basic subscriber account information.[66] If the subscriber is not authorized in the AuC, the phone will not be allowed to access the network.[67]

---

57. *Id.* at 13. It is also occasionally referred to as a handover, which is the standard European terminology. POOLE, *supra* note 13, at 58–59.

58. POOLE, *supra* note 13, at 76.

59. *Id.*

60. *See id.*

61. *Id.*

62. *Id.* at 59.

63. *Id.* at 62; SAUTER, *supra* note 23, at 12–13.

64. POOLE, *supra* note 13, at 62; SAUTER, *supra* note 23, at 12–14.

65. *See* POOLE, *supra* note 13, at 81; SAUTER, *supra* note 23 at 12–23.

66. *See id.* at 20. The AuC also stores individualized encryption keys that are utilized both during initial registration and to encrypt the content of communications. *Id.*

67. *See id.* at 20–23.

The PSTN is the backbone for public landline telephone services.[68] All telephone-based connections in the United States route back to the PSTN to provide interconnectivity amongst services.[69] It is through this connection that cell phones are able to call landline phones.[70] Since each network provider has a connection to the PSTN, this is also used to route data between network providers.[71]

HLRs and VLRs, the location registers, are used to track various subscriber information, including permitted network functions and the last-known location of every cell phone.[72] Every subscriber is tracked by their HLR, which is stored in one's "home" MSC.[73] If the subscriber uses his or her phone in a part of the network controlled by a different MSC, it will also be recorded in the VLR of that MSC.[74] The location registers record the last-known location of the subscriber to accurately forward incoming information to the subscriber.

c. The Intelligent Network

The intelligent network is non-essential for the actual operation of a cellular network.[75] It provides additional functionalities, such as managing prepaid services and other billing actions.[76] Essentially, this part of the network simply utilizes the data that is generated by the other sections of the physical network.

For instance, a common feature in the intelligent network is prepaid services. This feature functions by maintaining a registry

68. *See* Nadeem Unuth, *What is PSTN?*, LIFEWIRE (Oct. 7, 2016), https://www.lifewire.com/what-is-pstn-3426739.

69. *See id.*; POOLE, *supra* note 13, at 60.

70. POOLE, *supra* note 13, at 60.

71. *Id.*

72. *See* SAUTER, *supra* note 23, at 16–17; VELOCITY MADE GOOD LTD., A BRIEF GUIDE TO HLR LOOKUPS (Nov. 2014), https://www.hlr-lookups.com/open-downloads/a-brief-guide-to-hlr-lookups.pdf. Thus, every subscriber has a unique location register entry that includes the subscriber's identifying information on the network, current location, and a record of any supplementary services that the subscriber has access to. *See* SAUTER, *supra* note 23, at 16–17; VELOCITY MADE GOOD LTD., *supra*. Supplementary services include services such as call waiting, call forwarding, and conference calls. SAUTER, *supra* note 23, at 21 tbl. 1.4 (listing supplementary services and their functions).

73. *See* SAUTER, *supra* note 23, at 17. Typically, this is the MSC that encompasses the address given to the network provider when the cell phone was purchased.

74. *Id.* at 16.

75. *Id.* at 67.

76. *Id.*

of all prepaid cell phones that are used in the network and the amount of their prepaid minutes and/or text messages.[77] The prepaid services function will then monitor the network for activity from any prepaid cell phones through their unique identifying numbers.[78] When a call or a text message is identified, the appropriate amount of prepaid minutes or text message allotments is reduced in the registry.[79] Once a phone reaches zero, the prepaid services function can then interact with other parts of the network—such as the AuC—to disallow or alter the phones' ability to interact with the network.[80] Similar processes are used for other intelligent network functions, such as calculating roaming fees.[81]

2. Network Identifiers

Every network is broken down into increasingly smaller sections, which are each assigned identifying numbers. When compiled, these function as the physical address of each network component. The largest of these sections is known as the Mobile Country Code ("MCC"), which is a three digit number.[82] The first digit represents the geographical location of the country, while the next two digits identify the country.[83] For instance, the MCC of the United States is 310, with three representing North America.[84] Next, extremely large portions of a network are controlled by a singular MSC.[85] These large sections are identified by either a Mobile Network Code ("MNC") in GSM, or a System Identifier ("SID") in CDMA.[86]

---

77. *See id.*

78. *See id.* at 17–18.

79. *Id.* at 12.

80. *See id.* at 67.

81. *Id.* at 59.

82. *Id.* at 17.

83. *See id.* at 17–18.

84. *Id.* at 18; *Mobile Country Code*, OMICS INT'L, http://research.omicsgroup.org/index.php/mobile_country_code (last visited Feb. 13, 2017).

85. *See* SAUTER, *supra* note 23, at 12–13; POOLE, *supra* note 13, at 62. Often times, a service provider may only have one MSC for a small country. *See* TELECOMM. STANDARDIZATION BUREAU, INT'L TELECOMM. UNION, MOBILE NETWORK CODES (MNC) FOR THE INTERNATIONAL IDENTIFICATION PLAN FOR PUBLIC NETWORKS AND SUBSCRIPTIONS 4, 8, 11 (July 15, 2014), https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.212B-2014-PDF-E.pdf (showing small countries such as Aruba, Brumei Darussalam, and Cayman Islands to only have one MSC). However, large countries such as the United States have multiple MSCs per network provider. *See id.* at 53–60.

86. *See* VIJAY K. GARG, IS-95 CDMA AND CDMA2000: CELLULAR/PCS SYSTEMS

A single MSC is connected to a vast number of BSCs, each of which also receive an identifying number. In GSM, this number is called the Location Area Code ("LAC").[87] In CDMA, this number is referred to as the Network Identifier ("NID").[88] Lastly, while each BSC represents a relatively small geographical area, it still controls a number of individual base stations.[89] Each of these base stations also host multiple cells. The base stations and cells receive their own identifying number called a Cell Identifier ("CID") on GSM, or Base Station Identifier ("BID") in CDMA.[90]

3. Communications on Cellular Networks

All cellular networks utilize a form of Time Division Multiple Access ("TDMA") methodology.[91] This creates distinct time slots, or channels, which are used for particular network activities. For instance, there are discrete channels for establishing a network connection, synchronizing cell phones, or for making sustained data transmissions.[92] Cellular phones communicate on the proper channel according to what activity is taking place.[93]

Three types of channels are of immediate relevance: traffic channels, the access channel, and the paging channel. Traffic channels, as the name implies, are the channels where the network and cell phone pass significant amounts of data back and forth.[94] These channels are utilized for phone calls, text messaging, or receiving data for internet-based applications.[95]

IMPLEMENTATION 114 (2000); SAUTER, *supra* note 23, at 17.

87. *See* SAUTER, *supra* note 23, at 33, 52–53.

88. GARG, *supra* note 86, at 111, 114.

89. *See* SAUTER, *supra* note 23, at 27–28.

90. *See* GARG, *supra* note 86, at 117; SAUTER, *supra* note 23, at 52–53.

91. GSM networks break up frequencies into discrete time slots, while CDMA networks use a combination of different codes and time slots. *See supra* note 32.

92. *See* POOLE, *supra* note 13, at 85–86, 115–28 (listing different types of channels).

93. *See id.* at 84–86.

94. *See id.* at 86–88, 119.

95. In more technical terms, these data transmissions occur on different types of channels. For instance text messages are sent by the Short Message Service along the signaling path. *Id.* at 93. This means that they are sent on a separate channel known as the Standalone Dedicated Control Channel ("SDCCH"). *Id.* at 86. This channel is utilized for short bursts of data that do not require the continuous connection provided by a traffic channel. *See id.* Likewise, internet-based data may be sent differently depending on whether it is a short burst or a continuous transmission of data. However, for the purposes of this comment, these transmissions all function similarly and, for simplicity, are best grouped together as transmitting along a general traffic channel.

The access channel is used by cell phones to request a traffic channel in order to send or receive data.[96] The subscriber's cell phone sends a message to the network on the access channel, identifying the type of message it wants to send and requesting a traffic channel.[97] The network will receive the request and check to see if the cell currently providing service has an open traffic channel.[98] If it does, the cell phone will be assigned a traffic channel on that cell.[99]

The paging channel is used to deliver incoming messages to phones.[100] When the network has incoming data for a subscriber, it queries the location registers to find the last known location of that subscriber.[101] It then sends out a page—sometimes called a ping—on the paging channel of towers near that location.[102] When the subscriber's phone receives this page it responds to the network on the access channel.[103] From here, the process works just as setting up a data transmission. The phone identifies itself to the cell tower and then requests a time slot on a traffic channel.[104] The network assigns a traffic channel and then transmits the pending data.[105]

C. *What Is CSLI and Why Is It Generated?*

As the name implies, CSLI provides the location of the serving cell utilized in a network. More specifically, CSLI refers to a combination of information identifying a particular subscriber and the cell providing connectivity at a certain point in time.[106] Cellular networks record CSLI at various times for their own purposes.[107] There are no federal requirements to record this information.[108] However, coverage providers may include a clause in

96. *See id.* at 85, 125.
97. *See id.* at 90.
98. *See id.* at 131.
99. *Id.* at 91, 131.
100. *See id.* at 91.
101. *Id.*
102. *See id.*
103. *See id.* at 131.
104. *See id.*
105. *See id.*
106. *See* Christopher Fox, *Checking In: Historical Cell Site Location Information and the Stored Communications Act*, 42 SETON HALL L. REV. 769, 770–71 (2012).
107. *Id.* at 771.
108. *In re* United States for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).

their service contract detailing that it may collect location information and disseminate that information to third parties as required by law.[109]

CSLI is continuously created on cellular networks. Cell phones are programmed to report to their current serving cell every seven to nine minutes.[110] CSLI is generated each time this occurs.[111] Most pertinent though, CSLI can be generated when a cell phone communicates to a cell on the access channel.[112] This means every time a cell phone transmits or receives data, the network generates a CSLI data point. This includes every call, every text message, and every data request—from refreshing e-mail to loading a website. Even incoming data generates CSLI.[113] This is because the subscriber's cell phone will still automatically respond to a network page by communicating on the access channel.[114]

For the purposes of this comment, CSLI can be broken down into two categories: user-generated and non-user generated. User-generated CSLI refers to CSLI that is generated by the network in response to an event intentionally initiated by the subscriber. User-generated CSLI includes CSLI created when a subscriber turns his or her phone on, places a call, sends a text message, or uses the network to retrieve any other form of data, such as using the Internet or an internet-connected application.

On the other hand, non-user-generated CSLI refers to CSLI that is generated without any action by the subscriber. Non-user-generated CSLI comes in two varieties, periodic network updates and receiving calls and text messages. In both situations the subscriber's phone will automatically contact the network as long as it is connected, regardless of the subscriber's wishes.

Network providers collect CSLI in the normal course of business for a wide variety of internal business necessities.[115] All network providers record, at the very least, CSLI indicating the tower in which a particular connection was both initiated and

109. *See In re* United States Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1017 (N.D. Cal. 2015).

110. *See id.* at 1028

111. *See id.*

112. *See, e.g., id.* at 1027 (adjudicating that CSLI data points are generated not just by phone calls, but also by applications that send or receive data in the background).

113. *See id.* at 1028.

114. *See* POOLE, *supra* note 13, at 90–91, 131–32.

115. *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016).

terminated on.[116] Network providers may further collect CSLI for every cell used during a particular connection, instead of just the cell where the connection was initiated and terminated.[117]

The practice of collecting CSLI is not uniform amongst providers. Storing and maintaining CSLI records in databases comes at a cost, and each network provider makes individual decisions regarding how much CSLI and from which cellular interactions to record.[118] Network providers further make their own decisions on how long to maintain these records. However, at least one service provider records the CSLI generated from every periodic update.[119] This means that even when an individual never uses his or her phone, the government may still seek CSLI data points that were collected every seven to nine minutes, twenty-four hours a day.

D. *CSLI Accuracy*

CSLI accuracy is a hotly debated in CSLI litigation. Estimations of its accuracy range from being as inaccurate as a 3.5 square mile range[120] to within just meters.[121] The truth is dependent on individual circumstances, but rarely approaches either of these extremes. As described above, network providers structure their networks in accordance with the amount of users present in a specific location—more users equates to needing higher capacity, which in turn means more base stations and cells.

Accordingly, CSLI accuracy derives in large part from the area from which the information is drawn. In rural areas, CSLI may be inaccurate as the network may utilize only widely-spaced macro towers.[122] In such situations the accuracy of CSLI will be highly

116. *See, e.g.*, *id.* at 425; United States v. Davis, 785 F.3d 498, 502 (11th Cir. 2015) (en banc); In re *United States for Historical Cell Site Data*, 724 F.3d 600, 629 (5th Cir. 2013); *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 308 (3rd Cir. 2010).

117. *See* In re *United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 308.

118. *See* In re *United States for Historical Cell Site Data*, 724 F.3d at 612.

119. *In re* Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1028 (N.D. Cal. 2015) (noting that Sprint collects and records CSLI).

120. *See* United States v. Carpenter, 819 F.3d 880, 889 (estimating CSLI accuracy within 100 million square feet is equal to 3.587 square miles).

121. *See, e.g.*, *Davis*, 785 F.3d at 542 (quoting Brief for American Civil Liberties Union et al. as Amici Curiae at 9-10, United States v. Davis, 785 F.3d 498 (2015) (No. 12-12928)).

122. *See* POOLE, *supra* note 13, at 53.

unreliable and may equate to only a 120 degree sector spanning multiple square miles.[123] However, in modern times, these situations are the exception, not the rule.

The vast majority of investigations that utilize CSLI take place in densely occupied areas. A typical American city has a significant mixture of various base station types, due to network capacity needs.[124] Each of these base station types have varying coverage radii, but all are significantly smaller than rural macro towers.[125] Furthermore, higher tower density means that phones will conduct handoffs more often.[126] Each of these handoffs create additional CSLI points. This creates, in effect, a Venn diagram of location information. While an individual CSLI point may only identify a person within a square mile, two CSLI points collected from different cells a minute apart may have a much smaller overlapping coverage area.

Furthermore, technological advances have increased the potential accuracy of CSLI information. Network providers have the capability of recording more specialized information, such as the Angle of Arrival ("AoA").[127] The AoA designates the angle at which the radio wave hits the cell's antenna.[128] Thus, while CSLI only identifies a 120-degree radial wedge, by including AoA information, a network provider can greatly increase location accuracy. Additionally, by incorporating information about the strength of the signal received, location accuracy could be reduced further, to as low as thirty meters.[129]

Additionally, network providers may utilize a method called triangulation. With triangulations, multiple cells record information from a transmitting cell phone.[130] This information can

123. *See* Chris Silver Smith, *Cell Phone Triangulation Accuracy is All Over the Map*, SEARCH ENGINE LAND (Sept. 22, 2008), http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790; *see also* SAUTER, *supra* note 23, at 168.

124. *See supra* text accompanying notes 50–53.

125. *See supra* text accompanying notes 39–44.

126. *See supra* text accompanying notes 57–62.

127. *See* S.S. Bhandare & M.R. Dixit, *Positioning of Mobile in GSM Network Using Received Signal Strength and Angle of Arrival*, 2 INT'L J. EMERGING TRENDS & TECH. COMPUTER SCI. 400, 400 (2013), http://www.ijettcs.org/Volume2Issue3/IJETTCS-2013-06-24-122.pdf.

128. *See Angulation: AOA (Angle of Arrival)*, AALBORG U.: DEP'T ELECTRONIC SYS., http://kom.aau.dk/group/10gr891/methods/Triangulation/Angulation/ANGULATION.pdf (last visited Feb. 13, 2017).

129. *See* Bhandare & Dixit, *supra* note 127, at 403.

130. *See* Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Re-*

then be mapped out together, creating only a small area of overlap in which the cell phone must be located.[131] This method can be based on AoA technology, or on Time Difference of Arrival ("TDOA") technology.[132] Since all radio waves travel at the speed of light, the time in which a transmission takes to reach different towers can be used to approximate the distance from each tower.[133]

Each of these methods are utilized by network providers to comply with federal Enhanced 911 ("E911") standards. The E911 standards require that cell phone providers be able to identify cell phones within approximately 100 meters in the event of an emergency situation.[134] However, cell providers are not currently required to record this information, they need only be capable of generating it.[135] Hence, as with all CSLI, this more specific location information is recorded at the discretion of specific network providers.

E. *Law Enforcement's Collection of CSLI*

The broad umbrella of CSLI contains two distinct types of data: historical and prospective CSLI.[136] The most commonly sought is

---

garding the Use of Cellular Phones as Personal Locators, 18 HARV. J.L. & TECH. 307, 308 (2004).

131. *See id.* at 308–09; *see also In re* United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Tel., 460 F. Supp. 2d 448, 451 n.3 (S.D.N.Y. 2006).

132. Lockwood, *supra* note 130, at 308.

133. *Id.* at 308–09.

134. *See* Telecommunication, 47 C.F.R. § 20.18(h)(1)(i) (2015). The requisite accuracy differs to some extent because the E911 requirements are being initiated in phases with varied requirements in some areas. *See id.*

135. *See id.* § 20.18(h).

136. *See* R. Craig Curtis et al., *Using Technology the Founders Never Dreamed Of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 63 (2014). It is worth noting that law enforcement agencies are now capable of effectively cutting out the third party and unilaterally collecting CSLI information through use of cell-site simulators. *See, e.g.*, John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ (discussing state and local authorities' collection of cell-site information for investigative purposes); Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://www.wsj.com/articles/SB10001424053111904194604576583112723197574 (discussing federal authorities' use of one particular tool, a "stingray," to unilaterally obtain cell-site information in pursuit of a suspect). Like third-party CSLI, this form of active collection was originally conducted without a search warrant. However, current Department of Justice policy is to seek a search warrant absent specific criteria. *See* DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), https://www.jus

historical CSLI. Historical CSLI is simply the CSLI records that the provider has maintained for each subscriber.[137] Law enforcement can seek historical CSLI in one of two forms.

First, law enforcement can seek the historical CSLI data of a particular subscriber for a range of dates and/or times. This method of collection requires law enforcement to be able to identify a particular suspect and/or cell phone number.[138] However, it allows collection of CSLI for time frames beyond the physical commission of the crime.[139]

Second, law enforcement may seek what is known as a tower dump. With tower dumps, law enforcement does not request information about one subscriber from one network provider. Instead, it requests CSLI data for *all* phones that were connected to the cell, or cells, near the scene of a crime at the time it occurred.[140] Law enforcement may also then request tower dumps from *every* network provider in the area.[141] From this CSLI, law enforcement can identity subscriber identities and create a near-exhaustive list of individuals who were in the vicinity of the crime when it occurred.[142] Approximately 25 percent of all law enforcement agencies have utilized tower dumps.[143]

The second category is prospective CSLI. Prospective CSLI is when law enforcement asks the network provider to give real-time location updates so that they can locate an individual.[144] Network providers then actively direct law enforcement to the general vicinity of the individual.[145]

II. CSLI AND THE LAW

The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against

---

tice.gov/opa/file/767321/download.

137. *See* Curtis et al., *supra* note 136, at 63.

138. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).

139. *See, e.g., id.*

140. *See* Kelly, *supra* note 136.

141. *See, e.g., id.*

142. *See id.*

143. *Id.*

144. *See* Curtis et al., *supra* note 136, at 63; State v. Earls, 70 A.3d 630, 633–34 (N.J. 2013) (illustrating law enforcement's use of prospective CSLI).

145. *See, e.g., Earls*, 70 A.3d at 633–34.

unreasonable searches and seizures. . . ."[146] For the majority of the Fourth Amendment's history, it has been tied to common-law trespass.[147] However, the Supreme Court moved past this property-based approach in *Katz v. United States*, stating that "the Fourth Amendment protects people, not places."[148] *Katz* established that the Fourth Amendment protects a person's "reasonable expectation of privacy."[149]

"To fall within these protections, an expectation of privacy must satisfy 'a twofold requirement': first, the person asserting it must 'have exhibited an actual (subjective) expectation of privacy'; and second, that expectation must 'be one that society is prepared to recognize as "reasonable."' [150] The government's intrusion upon an area in which a person has a reasonable expectation of privacy constitutes a "search" under the rubric of the Fourth Amendment.[151] "[A]s a general matter, warrantless searches 'are *per se* unreasonable under the Fourth Amendment.'"[152]

It is under the basic rubric of *Katz* that the collection of CSLI is analyzed. However, by its nature, CSLI is at the intersection of two branches from the *Katz* tree: the third-party doctrine and Fourth Amendment law regarding physical location tracking. Part II.A–C examine the evolution of both of these doctrines and the significance that CSLI may indicate that one is at home—an area afforded extremely high constitutional protection.[153] Next, Part D will look to *Jones* and *Riley*, the Supreme Court's most recent forays into the Fourth Amendment and modern technology. Last, Part II.E. will look in-depth at the five circuits that have tackled the issue of historical CSLI to date.

---

146. U.S. CONST. amend. IV.

147. United States v. Jones, 565 U.S. 400, 405 (2012).

148. 389 U.S. 347, 351 (1967).

149. *Id.*; *Jones*, 565 U.S. at 406 ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'").

150. United States v. Carpenter, 819 F.3d 880, 886 (6th Cir 2016) (quoting *Katz*, 389 U.S. at 361 (Harlan, J. concurring)).

151. Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

152. City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (quoting *Katz*, 389 U.S. at 357).

153. *See* United States v. Karo, 468 U.S. 705, 714–15 (1984) (holding that "[s]earches and seizures inside a home without a warrant are presumptively, unreasonable absent exigent circumstances").

A. *The Stored Communications Act*

The Stored Communications Act ("SCA") is the statutory framework utilized by law enforcement to collect CSLI information.[154] Section 2703 of the SCA provides the means for law enforcement to gather various forms of electronic information from service providers. In particular, section 2703(c) applies to "a record or other information pertaining to a subscriber."[155] CSLI falls within this category of information.[156]

Section 2703(c) gives two options to obtain information in its purview: a search warrant pursuant to section 2703(c)(1)(A), or a court order under section 2703(c)(1)(B).[157] Court orders are governed under section 2703(d), which establishes the requisite standard.[158] To garner a section 2703(d) court order, law enforcement must offer "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[159] Courts have confirmed that section 2703(d)'s requirement of specific and articulable facts is less onerous than probable cause required by a warrant.[160]

B. *The Third-Party Doctrine*

The third-party doctrine stands for the general principle that an individual has no Fourth Amendment interest "in information he [or she] voluntarily turns over to third parties."[161] While this doctrine has roots in earlier precedent,[162] it was solidified by *Unit-*

154. 18 U.S.C. §§ 2701–2712 (2012 & Supp. 2016).

155. *Id.* § 2703(c).

156. *See In re* Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1016 (N.D. Cal. 2015) ("Although the SCA makes no mention of historical CSLI, there is no dispute that the historical CSLI sought by the government qualifies as a stored record or other information pertaining to a subscriber . . . or customer, and therefore falls within the scope of [section] 2703(c)(1).").

157. 18 U.S.C. § 2703(c).

158. *Id.* § 2703(d).

159. *Id.*

160. *See, e.g.*, United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015); *In re* United States for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013); *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315 (3rd Cir. 2010).

161. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

162. *See, e.g.*, Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 70 (1974); United States v. White, 401 U.S. 745, 749 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963).

ed States v. Miller.[163] In *Miller*, government officers subpoenaed a suspect's bank in order to obtain his bank records, including copies of original checks and deposit slips.[164] *Miller* expanded on *Katz*'s statement 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."[165] The Court emphasized that the information conveyed to the bank was not "confidential communications."[166] Instead, making clear that,

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[167]

Just three years later, the third-party doctrine came before the Court again, this time with regards to telephones. In *Smith v. Maryland*, a telephone company installed a pen register on a suspect's phones at the request of local police.[168] The pen register recorded the phone numbers that the suspect dialed in making telephone calls.[169] This information was then used as the basis, along with other evidence, to obtain a search warrant for the suspect's house.[170] In applying the *Katz* test, the Court held that the any subjective expectation of privacy the suspect may have had was not one that society was prepared to recognize as reasonable.[171] The Court rooted this conclusion firmly in the third-party doctrine, stating that "a person has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties."[172] The Court continued, observing that when the suspect used his phone he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[173] Especially pertinent to CSLI information, the Court noted that:

---

163. 425 U.S. 435 (1976).
164. *Id.* at 437–38.
165. Katz v. United States, 389 U.S. 347, 351 (1967); *see Miller*, 425 U.S. at 442.
166. *Miller*, 425 U.S. at 442–43.
167. *Id.* at 443.
168. 442 U.S. 735, 737 (1979).
169. *Id.*
170. *Id.*
171. *Id.* at 743.
172. *Id.* at 743–44.
173. *Id.* at 744.

> [t]he fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police.[174]

C. *The Fourth Amendment, Location Tracking, and the Sanctity of the Home*

The third-party doctrine is not the only relevant Supreme Court precedent regarding CSLI collection. Cell phones are generally carried with individuals everywhere they go. Setting accuracy questions aside, this allows law enforcement to use CSLI to have some ability to track movements of individuals as they move about their lives. This includes not only having a sense of where a person travels, but when that person's cell phone is at his or her house as well.[175] Accordingly, it is necessary to examine the leading cases on both location tracking and the special importance that one's home plays in Fourth Amendment inquiries.

United States v. Knotts provides the basic framework of location tracking jurisprudence, as well as the leading example for when the tracking of a person's location is not a search under the Fourth Amendment.[176] In *Knotts*, police officers placed a radio transmitter in a container of chloroform that was then transferred to the defendant.[177] Police officers used a combination of visual surveillance and the monitoring of the radio transmitter to track the container's movements to the defendant's home.[178] The Court recognized two critical facts: one, there was no evidence that the radio transmitter was monitored by police after it arrived at the defendants' house; and two, the tracking was confined to the container's movements on public roads.[179] The Court

174. *Id.* at 745.

175. For instance, in *Davis*, the government identified the defendant's "home" service cell tower, allowing an inference of the general area that the defendant's house was located in. United States v. Davis, 785 F.3d 498, 516 (11th Cir. 2015) (en banc). Notably, this allows the government to infer when the defendant spends the night somewhere besides his or her own home.

176. 460 U.S. 276, 277, 285 (1983).

177. *Id.* at 278.

178. *Id.*

179. *Id.* at 278–79, 281.

held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his [or her] movements from one place to another."[180]

Importantly, the Court left two questions unanswered in *Knotts*. First, the Court expressly avoided the defendant's contention that holding for the government would enable "twenty-four hour surveillance of any citizen of this country."[181] The Court clarified that "if such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[182] Second, the Court addressed only tracking on public roads, leaving open the possibility of a different result when it involves an area that historically receives higher levels of constitutional protection. The case addressing the second question came just one year later in *United States v. Karo*.[183]

Karo involved a similar set of circumstances to *Smith*. Police placed a beeper in one of the ten five-gallon drums of ether that the defendant had purchased from an informant.[184] Police monitored the beeper and used visual surveillance to track the container to the defendant's house.[185] Over the course of the next five months the police monitored the beeper periodically.[186] The police, using the beeper alongside traditional surveillance, tracked the container to six separate locations.[187] At times, the police also utilized the beeper to observe if the container was still present within the home of either the defendant or his accomplices.[188]

In *Knotts*, the beeper told the authorities nothing about the interior of the defendant's home.[189] Here, the Court made clear that monitoring the beeper revealed "a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a

180. *Id.* at 281.
181. *Id.* at 283.
182. *Id.* at 284.
183. 468 U.S. 705 (1984).
184. *Id.* at 708.
185. *Id.*
186. *Id.* at 708–10.
187. *Id.*
188. *Id.*
189. *Id.* at 705 (discussing United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

warrant."[190] In terms of the Fourth Amendment, the Court found no difference between using a beeper to confirm that property is located in a place withdrawn from visual surveillance, from that of an officer entering a place to confirm that fact—both are a search under the Fourth Amendment.[191] Since searches "inside a home without a warrant are presumptively unreasonable absent exigent circumstances," the Court found the monitoring of the beeper without a warrant to violate the Fourth Amendment.[192]

Although not dealing with location tracking, there is another key case that sheds light on the sanctity of the home in the age of modern technology. In *Kyllo v. United States*, police utilized a thermal imager to detect infrared radiation that was emanating from the defendant's house.[193] At the outset, the Court noted the particular problem presented by the technology in question. Historically, ordinary visual surveillance of a home was well within the bounds of police investigative techniques not requiring a warrant.[194] However, the technology at issue created a visual image out of non-visible infrared radiation, and thus its use constituted a search under the Fourth Amendment.[195]

In so holding, the Court espoused a number of principles relevant to a CSLI inquiry. Recognizing "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology," the Court framed the question as "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[196] The Court found unpersuasive the government's argument that the imaging did not "detect private activities occurring in private areas," but only "off-the-wall" radiation emanating from walls of the house.[197] Instead, the Court made clear that any

190. *Id.* at 715.

191. *Id.*

192. *Id.* at 714–15, 719.

193. 533 U.S. 27, 29–30 (2001). The police in *Kyllo* utilized this thermal imaging, without a warrant, to identify that certain parts of the defendant's house were radiating much higher levels of heat than the rest of his house, or any of the other homes in the triplex. *Id.* at 30. The police suspected that this indicated the use of halide lighting to grow marijuana. *Id.* Combining this information with tips from informants and utility bills, the police acquired a warrant to search the defendant's home, which revealed an indoor growing operation with more than 100 marijuana plants. *Id.*

194. *Id.* at 31–32.

195. *Id.* at 40.

196. *Id.* at 33–34.

197. *Id.* at 35, 37.

rule it adopts "must take account of more sophisticated systems that are already in use or in development."[198] Thus, although the technology used in *Kyllo* detected only "off-the-wall" infrared radiation, the Court was constrained by the possibility of technology that could detect "through-the-wall" infrared radiation, revealing the interior of the home.[199] A contrary holding could be seen to justify the use of "through-the-wall" thermal imaging, or comparable ultrasound technology, to detect specific details about the inside of a home from the road in front of it.[200]

D. *Modern Technology and Supreme Court Litigation*

Two recent Supreme Court decisions add to the doctrine. These decisions regard the current state of technology, the benefits it offers law enforcement, and the dangers it poses to Fourth Amendment privacy concerns. Although neither tackled the issue of CSLI, both shed light on how to balance old Fourth Amendment doctrine in the digital age.

1. *Jones*, the Mosaic Theory, and Location Tracking in the Digital Age

United States v. Jones[201] originated in the D.C. Circuit as *United States v. Maynard*.[202] Maynard and Jones appealed convictions following their joint trial for drug charges.[203] Jones challenged the use of location data collected by the police after attaching a GPS device to the undercarriage of his vehicle without a valid warrant.[204] This GPS device was used to monitor Jones's movements for twenty-four hours a day, for twenty-eight continuous days.[205] The D.C. Circuit began by addressing the question that *Knotts* squarely reserved: whether "dragnet-type law enforcement practices" would require the application of "different constitutional principles."[206]

198. *Id.* at 36.
199. *Id.*
200. *See id.*
201. 565 U.S. 400 (2012).
202. 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. on other grounds*, United States v. Jones, 565 U.S. 400 (2012).
203. *Maynard*, 615 F.3d at 548.
204. *Id.* at 555.
205. *Id.* at 558.
206. *Id.* at 556 (quoting Unites States v. Knotts, 460 U.S. 276, 283–84 (1983)).

The D.C. Circuit distinguished *Knotts*' holding: "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[207] The court explained,

> First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[208]

To support its theory of the whole being more than the sum of its parts, the court turned from Fourth Amendment law to the mosaic theory, which was developed with regards to Freedom of Information Act requests and national security information.[209] In those cases, the government often seeks to prevent the disclosure of information on the grounds that "[w]hat may seem trivial to the uniformed, may appear of great moment to one who has a broad view of the scene."[210]

After granting certiorari on the Fourth Amendment question in *Maynard*, the Supreme Court affirmed the D.C. Circuit's ruling on alternative grounds.[211] Justice Scalia penned the majority opinion, holding that the police violated the Fourth Amendment not under a *Katz* analysis, but under a property-based approach.[212] Having found there to be a warrantless physical trespass on private property, the Court refrained from addressing the constitutionality of the four-week GPS surveillance.[213]

Five justices, however, expressed concern over such long-term surveillance. Justice Sotomayor supplied the fifth vote in the majority opinion and wrote a separate concurring opinion that expressed her concern over the capabilities of digital surveillance,

---

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

208. *Maynard*, 615 F.3d at 558.

209. *Id.* at 562.

210. *Id.* at 562 (quoting CIA v. Sims, 471 U.S. 159, 178 (1985)).

211. United States v. Jones, 565 U.S. 400, 404 (2012).

212. *Id.* at 405, 408.

213. *Id.* at 412 ("Thus, even assuming that the concurrence is correct to say that traditional surveillance of Jones for a 4-week period would have required a large team of agents, multiple vehicles, and perhaps aerial assistance, our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

even if obtained "through lawful conventional surveillance techniques."[214] Location tracking methods may enable the government to "ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on."[215] Furthermore, these techniques come at a relatively low cost, and allow the government to "store such records and efficiently mine them for information years into the future."[216] In light of these concerns, Justice Sotomayor noted that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[217]

Justice Alito wrote for a four Justice minority; his concurrence echoed the concerns of Justice Sotomayor and the D.C. Circuit in regards to digital location tracking.[218] He argued the *Katz* formulation should have resolved the case rather than the majority's property-based approach.[219] Justice Alito emphasizes that a decision on reasonableness grounds would respect precedent regarding the "relatively short-term monitoring of a person's movements on public streets," because society has recognized that as reasonable.[220]

However, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[221] Although *Jones* involved only a GPS tracker, Justice Alito also invoked CSLI, referring to the practice of cell service providers to record location information which draws its accuracy from tower density.[222] Relatively easy and cheap access to such accurate and voluminous information is antithetical to traditional surveillance methods, which requires an unusually high expenditure of resources, serving as a check on its use.[223] The use of even crude location tracking technology removes some of these logistical restraints and increases the implications on the Fourth Amendment's protection of privacy.[224]

---

214. *Id.* at 416 (Sotomayor, J., concurring).
215. *Id.*
216. *Id.* at 415.
217. *Id.* at 417.
218. *Id.* at 418–19 (Alito, J., concurring in judgment).
219. *Id.* at 419.
220. *Id.* at 430.
221. *Id.*
222. *Id.* at 428.
223. *Id.* at 429.
224. *See id.* n.10 (noting that even the radio trackers used in *Knotts* and *Karo* allowed law enforcement to overcome significant logistical hurdles that would have—and in

2. *Riley*: The Impact of Cell Phone Technology on Fourth Amendment Doctrine

Riley v. California is the Supreme Court's most recent examination of modern technology under the Fourth Amendment.[225] *Riley* combined two separate cases[226] to examine the implications of cell phones on the search incident to arrest doctrine. In both cases police effectuated a valid arrest on the defendants and conducted a typical search incident to arrest which recovered, amongst other things, the defendants' cell phones.[227] Subsequent to the search the officers accessed, and later utilized, data on the cell phones.[228] At no point during the recovery of this data did the police obtain a search warrant.[229]

The government focused on *United States v. Robinson*.[230] In that case, the Court held that police officers were able to search a suspicious pack of cigarettes found during a lawful search incident to arrest.[231] The government argued that both the cigarette pack and the cell phone are containers, and searching one is "materially indistinguishable" from searching the other.[232] The Court responded by stating: "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[233]

The Court revealed a clear concern that unfettered law enforcement access to cell phone data goes far beyond the scope of the Court's pre-digital decisions. Echoing the mosaic theory concerns from *Jones*, the Court noted that "a cell phone's capacity allows even just one type of information to convey far more than

---

Knotts, in fact did—inhibit traditional surveillance techniques).

225. 134 S. Ct. 2473 (2014).

226. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013); People v. Riley, No. S209350, 2013 LEXIS 3714 (Cal. 2013).

227. *Riley*, 134 S. Ct. at 2480–81.

228. *Id.* at 2480–82.

229. *Id.*

230. United States v. Robinson, 414 U.S. 218 (1973).

231. *Riley*, 134 S. Ct. at 2488–89. In *Robinson*, a police officer conducted a search incident to arrest and found a crumpled pack of cigarettes with an item in side that did not feel like cigarettes. 414 U.S. at 221–23. The officer opened the pack of cigarettes and found heroin capsules inside. *Id.* at 223. The Court subsequently upheld this action as valid under the search incident to arrest doctrine. *Id.* at 236.

232. *Riley*, 134 S. Ct. at 2488.

233. *Id.*

previously possible."[234] The sum of an individual's private life can be reconstructed using even one type of data from a cell phone.[235] The Court also expressed a continued unease with modern location data, noting that "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[236]

The Court recognized that modern cell phones cannot be simply analyzed under outdated rubrics. Instead, cell phones must be understood with an eye to their unique uses, capabilities, and implications. With all that cell phones may contain and reveal, "they hold for many Americans the privacies of life."[237] Accordingly, the Court held that the search of a cell phone seized incident to arrest requires a warrant, absent exigent circumstances.[238]

E. *The Confusion in Applying Ill-Suited Precedent to CSLI*

Five circuits to date have addressed the issue of historical CSLI collection. All have applied the third-party doctrine to CSLI.[239] Although the Third Circuit held that CSLI was not disclosed voluntarily,[240] it is the outlier. The Fourth, Fifth, Sixth, and Eleventh Circuit have all held that historical CSLI is not subject to Fourth Amendment protections via application of the third-party doctrine.[241] However, this majority is not as clean as it appears. In the Eleventh and the Fourth Circuits, the original three judge panel held opposite, only to be vacated and overruled en banc.[242] Each of these four circuits have also seen vigorous dissent.[243] They

234. *Id.* at 2489.

235. *See id.* at 2489–90.

236. *Id.* at 2490 (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

237. *Id.* at 2494–95 (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

238. *Id.* at 2494–95.

239. United States v. Graham, 824 F.3d 421, 437-38 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 889-90 (6th Cir. 2015); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013); *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010).

240. In re *United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 319.

241. *See supra* note 1 and accompanying text.

242. *See supra* note 2 and accompanying text.

243. *See supra* note 3 and accompanying text.

serve to show not only that multiple lines of Fourth Amendment precedent dictate different results, but that each of those lines are archaic and in desperate need of revision in today's digital age.

1. *In re United States Directing a Provider of Electronic Communication Service to Disclose Records to the Government*

The Third Circuit was the first to hear a challenge to the collection of historical CSLI data. The case arose from Magistrate Judge Lenihan's denial of the Government's request for a Stored Communications Act ("SCA") order compelling a network provider to turn over historic CSLI data.[244] Judge Lenihan held that the historical CSLI data is protected by the Fourth Amendment, thus requiring a showing of probable cause.[245] In an unusual step, each of the other four Magistrate Judges of the Western District of Pennsylvania also signed onto the opinion of Judge Lenihan.[246] Judge Lenihan's opinion was subsequently affirmed by the District Court.[247]

The Third Circuit began with an examination of the utilized provisions of the SCA and held that CSLI was obtainable under a section 2703(d) court order.[248] The court further clarified that section 2703(d) orders require only an intermediate standard, higher than that of a subpoena, but lower than probable cause.[249] Reaching the core of the case, the court examined the SCA's statutory scheme as a whole, attempting to decipher the SCA's option of obtaining either a warrant under section 2703(c)(1)(A) or a court or-

244. *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 589 (W.D. Pa. 2008).

245. *Id.* at 616.

246. *See id.*; *see also In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308 (3rd Cir. 2010) ("We note, preliminarily, that the [magistrate judge's] opinion was joined by the other magistrate judges in that district. This is unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues who, after all, routinely issue warrants authorizing searches and production of documents.").

247. *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, No. 07-524M, 2008 U.S. Dist. LEXIS 98761, at *3 (W.D. Pa. Sept. 10, 2008).

248. *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv., 620 F.3d at 313.

249. *Id.* at 314 (examining the legislative history of the SCA).

der pursuant to section 2703(d).[250] The government argued that the prosecutor has discretion between the two choices, while Judge Lenihan had held that a magistrate judge has the option to require either based on the constitutional interests in the information sought.[251] The court rejected the government's argument, in large part due to its "[concern] with the breadth of the Government's interpretation of the statute that could give the Government the virtually unreviewable authority to demand a [section] 2703(d) order on nothing more than its assertion."[252] Thus, "[t]he Government's position would preclude magistrate judges from inquiring into the types of information that would actually be disclosed by a cell phone provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment."[253]

The Third Circuit outright rejected the government's assertion that no CSLI can implicate Fourth Amendment protections due to the third-party doctrine.[254] Instead, the court found the amicus brief of the Electronic Frontier Foundation ("EFF") persuasive, noting:

> A cell phone customer has not voluntarily shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.[255]

However, none of the court's reasoning was a holding, per se. In the end, the Third Circuit vacated the opinion of Judge Lenihan because she never analyzed whether the Government made a proper showing under section 2703(d) of the SCA.[256] The court vacated the opinion and remanded the case for the magistrate judge to develop a factual record identifying whether the Government

250. *Id.* at 316–17.
251. *Id.* at 316.
252. *Id.* at 317.
253. *Id.*
254. *Id.* at 317–18.
255. *Id.* at 317–18.
256. *Id.* at 319.

satisfied their burden under section 2703(d).[257] After that determination, the court left the magistrate free to investigate the information sought and make a discretionary choice as to whether the heightened requirement of a probable cause showing was called for in light of constitutional concerns.[258]

Up to this point, the third-party doctrine had mentioned only voluntary conveyance to a third party. The idea that a person voluntarily and knowingly conveys information to a third party introduces the concept of both knowledge and purpose to the doctrine. This in no way conflicts with precedent, where defendants voluntarily, knowingly, and purposely conveyed their bank records, or the phone numbers they dialed.[259] However, these concepts are an addition to the strict reading of the doctrine and provide important implications on the third-party doctrine with which future circuits would struggle.

2. *In re United States for Historical Cell Site Data*

The Fifth Circuit took up the issue of historical CSLI just three years later and substantially departed from the rationale behind the Third Circuit's opinion. The issue was also appealed from a denial of a section 2703(d) order; this case consolidated three denials.[260] As an initial matter, the Fifth Circuit held that section 2703(d) of the SCA did not grant magistrate judges the discretion to require a showing of probable cause if the statute's requirements were otherwise met.[261] In so holding, the court narrowed the relevant question to the constitutionality of section 2703(d) orders as applied to historical CSLI data.[262]

To no surprise, the opposing parties framed the issue along distinct lines of precedent: the Government focused on the third-party doctrine and the American Civil Liberties Union ("ACLU") on location tracking.[263] The court found the defining question to be

257. *Id.*

258. *Id.*

259. Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (knowingly dialing phone numbers); United States v. Miller, 425 U.S. 435, 442 (1976) (voluntarily conveying bank documents).

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

261. *Id.* at 606–07.

262. *See id.* at 607.

263. *Id.* at 608.

who is recording the information.[264] The Fifth Circuit held that CSLI is "clearly a business record" falling within the scope of the third-party doctrine because it is a record of a transaction to which the record-keeper was a party.[265]

The ACLU put forth a similar argument to the one found persuasive by the Third Circuit: that a subscriber directly conveys only the number dialed, not the CSLI.[266] The court summarily dismissed this "crabbed understanding of voluntary conveyance," because it claimed it would lead to absurdities.[267] It elaborated that a user who programmed a number into speed dial would then presumably be considered to convey only the "speed dial reference number."[268] This result may arguably flow from a requirement of direct conveyance. However, it wholly neglects the fact that using speed dial would still mean that a subscriber voluntarily, knowingly, and purposely conveyed the full telephone number to network provider.

Despite this, the Fifth Circuit found that cell phone users voluntarily convey their CSLI by the voluntary use of their cell phones.[269] Thus, the third-party doctrine controlled and no search occurred. The court found that the SCA—despite being passed in 1986, long before ubiquitous use of cell phones—was the legislative solution to balancing Fourth Amendment interests in CSLI data against law enforcement needs.[270] The court did make clear, however, that it was holding only that CSLI collection under section 2703(d) was not categorically unconstitutional.[271] It left open the possibility that section 2703(d) may be unconstitutional as applied to specific instances of CSLI.

264. *Id.* at 610.

265. *Id.* at 611.

266. *Id.* at 613 (citing *In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (2010) ("[W]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed. . . .").

267. *Id.*

268. *Id.*

269. *Id.*

270. *Id.* at 614–15.

271. *Id.* at 615.

3. *United States v. Davis*

Davis was the first court to rule on a defendant's motion to suppress CSLI collected without a warrant. The District Court denied both Davis's motion to suppress prior to trial and his renewed motion during trial.[272] The three judge panel framed the question presented as whether Fourth Amendment protections cover not only the content of the defendant's electronic transmissions, "but also the transmission itself when it reveals information about the personal source of the transmission, specifically his location."[273]

Finding *Jones* instructive, although not controlling, the panel used it to guide their analysis.[274] The panel agreed with the Government that CSLI is distinguishable from the GPS data at issue in *Jones*, however it found that the distinction worked against the government.[275] The panel noted that the GPS data in *Jones* revealed publically available information, and was thus protectable under either the property-based theory of the majority or the concurrences' aggregate data theory.[276] Conversely, the panel stated, "even one point of cell site location data can be within a reasonable expectation of privacy," making it "more like communications data than it is like GPS information."[277]

The panel also rejected the Government's assertion that CSLI is less protected than GPS data purely because it lacks the precision of GPS data.[278] The panel agreed that this may be the case, but asserted that the point has no constitutional significance.[279] The Government had undercut this theory, stressed the panel, by emphasizing at trial that CSLI placed the defendant near the scene of the crimes.[280] This was materially no different than placing a person near the "home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."[281]

---

272. United States v. Davis, 754 F.3d 1205, 1209 (11th Cir. 2014), *vacated*, 573 F. App'x 925 (11th Cir. 2014) (Mem.).

273. *Id.* at 1213.

274. *Id.* at 1215 (discussing United States v Jones, 565 U.S. 400 (2012)).

275. *Id.*

276. *See id.* at 1215–16.

277. *Id.* at 1216.

278. *Id.*

279. *Id.*

280. *Id.*

281. *Id.*

Lastly, the panel rejected the proposition that the third-party doctrine applies. It found the Third Circuit's rationale persuasive, that CSLI is not voluntarily conveyed.[282] To buttress this position, the panel used the Government's own closing argument to the jury "that obviously Willie Smith, like [Davis], probably had no idea that by bringing their cell phones with them to these robberies, they were allowing [their cell service provider] and now all of you to follow their movements on the days and at the times of the robberies. . . ."[283]

This opinion of course, was vacated in lieu of an en banc hearing in which the court held nine to two that the third-party doctrine applied and no Fourth Amendment violation occurred.[284] It is worth noting however, that two of the panel's judges did not participate in the en banc hearing.[285] The court's holding was evident from its framing of the question presented: "whether the court order authorized by [section 2703(d) of the SCA], compelling the production of a third-party telephone company's business records containing historical cell tower location information, violated Davis's Fourth Amendment rights. . . ."[286]

The court focused on the Supreme Court's holding in *Smith v. Maryland*,[287] where the defendant had revealed information from the constitutionally protected area of his house, as juxtaposed to the use of a cell phone outside of one's house.[288] The court viewed *Smith* as presenting a stronger argument for Fourth Amendment protection than *Davis*—despite the Government receiving 11,606 separate location data points over the course of sixty-seven days.[289] The Eleventh Circuit also looked to *In re United States for Historical Cell Site Data* for support for its holding that the de-

282. *Id.* at 1216–17.

283. *Id.* at 1217.

284. United States v. Davis, 573 F. App'x 925 (11th Cir. 2014) (Mem.) (vacating panel decision and granting an en banc hearing); United States v. Davis, 785 F.3d 498, 518 at n.21 (11th Cir. 2015) ("Nine members of the en banc court agree there was no Fourth Amendment violation in this case.").

285. Judge David Bryan Sentelle of the D.C. Circuit sat by designation on the panel. *Davis*, 754 F.3d at 1208. Judge Joel F. Dubina elected not to participate in further proceedings under 28 U.S.C. § 46(c). *Davis*, 573 F. App'x at 925.

286. *Davis*, 785 F.3d at 500, *cert. denied*, Davis v. United States, 136 S. Ct. 479, 480 (2015).

287. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

288. *Davis*, 785 F.3d at 508.

289. *Id.* at 508; *id.* at 533 (Martin, J., dissenting).

fendant had no reasonable expectation of privacy in the CSLI in question because of the third-party doctrine.[290]

Last, the court addressed the concerns over technological advancement and the holding in *Jones*. While acknowledging that technology here far surpasses that at issue in cases such as *Smith*, the majority considered these concerns as being better directed to Congress and state legislatures.[291] The majority then proceeded to explain that the *Jones* concurrences did not impact the case, noting that neither Justice Sotomayor nor Justice Alito's concurrences came close to overturning the third-party doctrine, leaving *Smith* and *Miller* as the controlling law.[292]

Curiously, the court did go on to note that "[w]ithout question, the number of calls made by Davis over the course of 67 days could, when closely analyzed, reveal certain patterns with regard to his physical location in the general vicinity of his home, work, and indeed the robbery locations."[293] It continued, stating that the record presented no evidence that the CSLI in question produced anything near an intimate portrait of the defendant's life.[294] The court offered no explanation as to why CSLI, if capable of revealing patterns of the defendant's location in the vicinity of his home and work, did not implicate the five concurring Justices' concerns in *Jones* that patterns could be used to reveal a wealth of other private details that may implicate the Fourth Amendment through their aggregation.[295]

4. *United States v. Carpenter*

United States v. Carpenter arose in similar circumstances to those present in *Davis*: the Government collected historical CSLI without a warrant, placing the defendant in the vicinity of a number of robberies he was charged with.[296] The three judge panel centered its analysis on a derivative concept of the third-party

290. *Id.* at 509–11 (discussing *In re* United States for Historical Cell Site Data, 724 F.3d 600, 611–15 (5th Cir. 2013)).

291. *Id.* at 512.

292. *Id.* at 514.

293. *Id.* at 516.

294. *Id.*

295. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *id.* at 428–29 (Alito, J., concurring).

296. United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).

doctrine; although the content of communications is protected, the information necessary to route it is not.[297]

This theory emerges from cases that long pre-date the construction of the third-party doctrine. In *Ex parte Jackson*, the Supreme Court ruled that although the contents of a letter are protected, the addresses on the outside of the envelope enjoy no such Fourth Amendment protections.[298] The panel framed *Smith v. Maryland* similarly, as the recorded numbers were the routing information necessary to make a call.[299] Last, it notes that circuit courts have used similar logic in protecting the contents of an e-mail, but not the IP addresses and metadata necessary to route the e-mail to its destination.[300] The panel stated that CSLI is similar to these kinds of routing information, holding that "[t]he government's collection of business records containing these data therefore is not a search."[301]

The panel then moved to the argument of the defendants and the ACLU that *Jones* liberated the court from following the third-party doctrine.[302] Setting aside the fact that *Jones*'s concurrences are not controlling, the panel proceeded to distinguish CSLI and GPS data based on their respective accuracies.[303] According to the panel, the CSLI in question is only accurate "within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the GPS data in *Jones*."[304] This may be true of a single cell, taken out of the context of a network provider's infrastructure. However, modern cells provide coverage to much smaller areas in order to maximize network capacity.[305] Additionally, the panel did not question why, if the data is so wildly inaccurate, law enforcement and prosecutors consistently utilize it to place defendants in the immediate vicinity of a crime.

Last, the court dismissed the defendant's arguments centered on *Riley*. It found no connection between the data at issue in *Riley*

297. *Id.* at 886.

298. *Ex parte* Jackson, 96 U.S. 727, 733 (1878); *Carpenter*, 819 F.3d at 886 (explaining *Ex parte* Jackson and its significance).

299. *Carpenter*, 819 F.3d at 887 (discussing Smith v. Maryland, 442 U.S. 735 (1979)).

300. *Id.*

301. *Id.*

302. *Id.* at 888.

303. *Id.* at 889.

304. *Id.*

305. *See supra* text accompanying notes 50–53.

and CSLI; stating that Congress already passed a statutory scheme balancing government interests and Fourth Amendment protection of CSLI when it passed the SCA.[306] Of course, the panel did not explain how this balance was struck before widespread cell phone usage in 1986, when the SCA was passed.

Judge Stranch concurred only in judgment with the panel's treatment of CSLI, finding that the good faith exception operates regardless of the outcome of the Fourth Amendment question.[307] Judge Stranch wrote separately to express his concerns over the current state of the law with regards to CSLI. Echoing Justice Sotomayor's concurrence in *Jones*, Judge Stranch wrote:

> It seems to me that our case resides at the intersection of the law governing tracking of personal location and the law governing privacy interests in business records. This case involves tracking physical location through cell towers and a personal phone, a device routinely carried on the individual's person; it also involves the compelled provision of records that reflect such tracking. . . . I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location. And it seems to me that the business records test is ill suited to address the issues regarding personal location that are before us.[308]

Judge Stranch noted the comparative inaccuracy of CSLI compared to GPS data, but maintained that extensive tracking, even through CSLI, implicates serious Fourth Amendment concerns.[309] CSLI may not be as precise as GPS data, but it is far from "innocuous routing information."[310] These simple facts led Judge Stranch to conclude that it was necessary to develop a new test to determine when a warrant is necessary for the collection of records indicating personal location.[311] Such a test, according to Judge Stranch, ought to place at least some limitation on either the quantity of records or length of time for which such records may be compelled.[312]

---

306. *Carpenter*, 819 F.3d at 889 (discussing Riley v. California, 134 S. Ct. 2473, 2473–85 (2014)).

307. *Id.* at 893–94 (Stranch, J., concurring).

308. *Id.* at 895.

309. *Id.*

310. *Id.*

311. *Id.* at 895–96.

312. *Id.* at 896.

5. *United States v. Graham*

The Fourth Circuit is the most recent court to rule on the collection of historical CSLI. *United States v. Graham* first reached the court in 2015 after a district court had ruled that the defendant had no expectation of privacy in the CSLI under the third-party doctrine.[313] The three judge panel reversed, finding two-to-one that the third-party doctrine did not apply.[314] As an initial matter, the court pointed out that the third-party doctrine does not immunize all third-party records from the protections of the Fourth Amendment.[315] More saliently though, the Court rejected the notion that a subscriber voluntarily conveys CSLI to their network provider.[316]

In doing so, the court focused on voluntary conveyance in an active sense. The court found that the user is not required to submit the location information, but that the "service provider automatically generates CSLI in response to connections made between the cell phone and the provider's network, with and without the user's active participation."[317] The panel's majority expressly endorsed the reasoning of the Third Circuit and rejected that of the Fifth and Eleventh Circuits.[318]

Following an en banc rehearing, Judge Motz, the panel's dissenting judge, wrote for a 12-4 majority in an opinion that largely reiterated her dissent.[319] Perhaps revealing its discomfort with the outcome, the court held that "without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment."[320] However, the opinion drew direct parallels to *Smith*, noting that in both cases the defendant "exposed" the relevant information to the phone company's "equipment in the ordinary course of business."[321] The court buttressed its holding by noting that not only did this decision adhere to those of the Fifth,

313. United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Md. 2012), *aff'd*, 824 F.3d 421, 422 (4th Cir. 2016) (en banc).

314. United States v. Graham, 796 F.3d 332, 338, 352 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

315. *Id.* at 351–52 ("The precedents of this Court and others show that a Fourth Amendment search may certainly be achieved through an inspection of third-party records.")

316. *Id.* at 354, 354 n.14.

317. *Id.* at 354.

318. *Id.* at 355.

319. United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (en banc).

320. *Id.* at 425.

321. *Id.* at 427 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

Sixth, and Eleventh Circuits, but to the "vast majority of federal district court[s]."[322]

The court squarely rejected the contention that the CSLI conveyance was compulsory, not voluntary.[323] Similarly, it found unpersuasive that subscribers lack knowledge of CSLI to voluntarily convey.[324] It agreed with the Sixth Circuit's logic in *Carpenter*, that all subscribers have at least some basic awareness that their location is both important and utilized in network connectivity.[325] The court took their reasoning a step further, however, noting that voluntarily "does not require contemporaneous recognition of every detail an individual conveys to a third party."[326] Instead, the court noted that the third-party doctrine applies in all instances except where an individual "*in*voluntarily conveys information."[327]

III. REEXAMINING THE RESULTS OF THE THIRD-PARTY DOCTRINE

The third-party doctrine's applicability turns on two novel distinctions. First, whether information that is not actively disclosed be conveyed under the meaning of the Fourth Amendment. Second, whether it is voluntarily conveyed, assuming this information falls under the ambit of information exposed to a third party. Contrary to the bulk of circuit court opinions, this comment posits that a strict application of the third-party doctrine leads to a fractured result: user-generated CSLI is subject to the third-party doctrine, while non-user-generated CSLI is not.

This convoluted result fails to either fully protect privacy or advance the interests of law enforcement. More distressing, it forces courts into the untenable position of needing to become subject matter experts in complicated technology. Like *Riley* and *Jones*, it is time for the Supreme Court to modify doctrine that no longer fits our digital world.

322. *Id.* at 428, 428 n.6 (noting multiple federal district courts that reached the same conclusion).

323. *Id.* at 429.

324. *Id.*

325. *See id.* (citing United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016)).

326. *Id.* at 430.

327. *Id.* at 430–31.

A. *A Strict Application of the Third-Party Doctrine to CSLI*

To answer the question of voluntary conveyance it becomes necessary to find a working definition of both words. Prior to the digital age, it was not necessary to define voluntary conveyances beyond their ordinary and plain meaning. In *Miller*, the defendant walked into a bank and physically handed the documents in question to a bank employee.[328] In *Smith*, the defendant picked up a phone and physically dialed the numbers in question.[329] Both were obvious voluntary actions and plainly constituted a conveyance of information.

CSLI presents novel issues, however. For instance, a cell phone user is, for all intents and purposes, never aware of which cell he or she is utilizing for network coverage.[330] Is it even possible for a person to convey information that he or she does not know? Cell phones, likewise, never actually transmit CSLI information. Rather, CSLI information is generated when cell phones make a connection with the network.[331] Similarly, if there is a conveyance, how should courts decide if it was voluntary? On one end of the spectrum, voluntariness connotes purpose and knowledge; on the other, voluntary may mean only a lack of coercion.

1. Defining Conveyance

The general rule underpinning the third-party doctrine is that a person has no legitimate expectation of privacy in information he or she voluntarily conveys to third parties.[332] Despite having never needed to define a "conveyance," the Supreme Court has found occasion to use a number of synonyms that shed light on its meaning for purposes of Fourth Amendment analyses. For instance, the Supreme Court has referred to voluntary conveyances as one "revealing his affairs to another";[333] "voluntarily turn[ing]

328. United States v. Miller, 425 U.S. 435, 442 (1976).

329. Smith v. Maryland, 442 U.S. 735, 743 (1979).

330. There are phone applications which may be utilized to display this data, but they certainly are not commonly used. *See, e.g.*, *Network Cell Info Lite*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.wilysis.cellinfolite&hl=en (last visited Feb. 13, 2017).

331. *See supra* Part I.C.

332. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

333. United States v. Miller, 425 U.S. 435, 443 (1976); *accord* Smith v. Maryland, 442 U.S. 735, 744 (1979) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . .").

over [information] to third parties";[334] and "knowingly expos[ing] [information] to the public."[335]

The verb to "convey" is defined as "[t]o transfer or deliver."[336] Thus a conveyance, in common parlance, would require an active action by the conveyor. However, the Supreme Court's use of words such as "revealing" and "exposing" demonstrates an intention for conveyances to be viewed as incorporating more than this standard definition entails. By utilizing these words the Supreme Court has indicated that conveyances, under the Fourth Amendment, should be viewed as including information that an individual makes available to some third party.

Defining a conveyance as simply making information available provides a much more coherent understanding of Fourth Amendment doctrine than an active definition would. Although either definition would be applicable in *Miller* and *Smith*, the same is not true of other third-party doctrine cases. For instance, in cases involving trash left in public areas, a strict reading of conveyance as a direct transfer would be problematic. Instead, the Supreme Court's holdings that trash left in public areas is not protected by the Fourth Amendment are better understood as the defendant having made that trash available to a third party—be that placing it a public refuse bin[337] or placing household trash at the curb.[338] This is especially true, as law enforcement in those cases directly inspected the trash before it ever made it to the third party.[339] If the Supreme Court required a direct conveyance to the third party before Fourth Amendment protections were removed, then any discussion of the third-party doctrine in these cases would be superfluous.

Utilizing this standard to examine CSLI, it is clear that it constitutes a conveyance under the Fourth Amendment. The fact that an individual does not know his or her exact CSLI information would be problematic with a definition of conveyance requiring some direct transfer of information. However, defining a conveyance as making information available alleviates this problem. A person need not be aware of exact information to make it available to others. For instance, a person is likely not aware of

334. *Smith*, 442 U.S. at 743–44.
335. California v. Rooney, 483 U.S. 307, 322 (1987) (per curiam).
336. *Convey*, BLACK'S LAW DICTIONARY (8th ed. 2004).
337. *See Rooney*, 483 U.S. at 307.
338. *See* California v. Greenwood, 486 U.S. 35, 35 (1988).
339. *Greenwood*, 486 U.S. at 37; *Rooney*, 483 U.S. at 309.

every piece of information that is contained in his or her garbage. Yet, every piece of that information is considered conveyed by placing it on the curb to be picked up.[340]

Likewise, when a person utilizes a cell phone, the network provider receives information regarding the cell that the person is connecting through.[341] For the purposes of analyzing the existence of a conveyance, it is of no importance that the individual is unaware of the exact CSLI being made available.

2. When Is a Conveyance Voluntary?

As with "conveyance," the Supreme Court has not had occasion to define the word "voluntary" within the context of the Fourth Amendment. The word has two separate definitions: an action "[d]one by design or intention," or an action "[u]nconstrained by interference; not impelled by outside influence."[342] Likewise, courts and litigants have espoused two general definitions. The Third Circuit and non-government litigants have defined "voluntary" as requiring affirmative action done with knowledge of the results.[343] The contrary definition is that voluntary equates to anything that is not coercive.[344]

The proper definition of voluntary, however, becomes clear from examination of its context in Fourth Amendment precedent.

340. *See Greenwood*, 486 U.S. at 40.

341. *See supra* Part I.C.

342. *Voluntary*, BLACK'S LAW DICTIONARY (8th ed. 2004).

343. *See In re* United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, '[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.'"); *see also In re* United States for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (describing the ACLU's arguments in the same terms as the Third Circuit's holding); United States v. Graham, 824 F.3d 421, 429 (4th Cir. 2016) (en banc) ("Defendants . . . argue that '[a] cell phone user does not even possess the CSLI to voluntarily convey,' and that even assuming users do convey such information, 'revealing this information is compelled, not voluntary.'").

344. *See, e.g.*, *Graham*, 824 F.3d at 430–31 ("[T]he Supreme Court's use of the word 'voluntarily' in *Smith* and *Miller* does not require contemporaneous recognition of every detail an individual conveys to a third party. Rather, these cases make clear that the third-party doctrine does not apply when an individual *in*voluntarily conveys information . . . .").

The phrase "voluntary conveyance" was first utilized in *United States v. Miller*.[345] The court began with *Katz*'s statement of law that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[346] Only in examining whether the bank documents were knowingly exposed did the Court then note that the documents obtained contained "only information voluntarily conveyed to the banks and *exposed* to their employees in the ordinary course of business."[347] This sentence makes clear that the Court viewed "voluntary conveyance" to be synonymous to exposing information. It is hard to fathom that the Court was impliedly reading out *Katz*'s requirement of knowledge just a few sentences after stating it as controlling precedent.[348]

Since *Miller*, the Court has been ambiguous regarding a voluntary knowledge requirement. *Smith*, for instance, did not quote *Katz* for this proposition, and thus no version of knowledge is present in that section of the opinion.[349] Instead, *Smith* quoted *Miller* for the above sentence, that Miller had "no 'legitimate expectation of privacy' in financial information 'voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business.'"[350] *Smith* then goes on to draw an exact parallel, stating that the petitioner "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[351] Thus, despite omitting the word knowingly, *Smith* maintained the synonymous nature of voluntary conveyance and exposure from *Miller*. Since *Miller*'s use of the word "exposure" was based on *Katz*'s requirement of "knowing exposure," the component of knowledge is fairly imputed to the *Smith* opinion as well.

Other Supreme Court opinions however, have demonstrated the continuing vitality of *Katz*'s "knowing exposure" requirement. In *Rooney*, the defendant had placed betting papers in a communal trash bin that was then put in his apartment basement to be picked up.[352] In explaining why certiorari should be granted, the

345. 425 U.S. 435 (1976).
346. *Miller*, 425 U.S. at 442 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).
347. *Id.* (emphasis added).
348. *See id.*
349. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
350. *Id.* at 744 (citing *Miller*, 425 U.S. at 442).
351. *Id.*
352. California v. Rooney, 483 U.S. 307, 308 (1987) (per curiam).

dissent began by noting *Katz*'s statement that knowing exposure to the public removes potential Fourth Amendment protections.[353] The dissent continued, stating:

> Respondent knowingly exposed his betting papers to the public by depositing them in a trash bin which was accessible to the public. Once they were in the bin, he no longer exercised control over them. . . . Indeed, he placed his papers in the bin for the express purpose of conveying them to third parties, the trash collectors, whom he had no reasonable expectation would not cooperate with the police.[354]

The dissent then elaborated on the holding of *Smith*, repeating that respondent had "no legitimate expectation of privacy in information he voluntarily turns over to third parties."[355]

The consistent intermingling of *Smith* and *Miller*'s formulation of the third-party doctrine and *Katz*'s original notion of knowing exposure to the public are not distinct and separate. Rather, the third-party doctrine's concept of voluntary conveyance includes the requirement of knowing exposure. Certainly, as the Fourth Circuit noted, contemporaneous knowledge of every detail is not necessary to satisfy the requirement that a voluntary conveyance is done knowingly.[356] Otherwise, the government would be required to show that the individual knew every piece of information contained in his or her trash can—an impossible task. However, these cases demonstrate that the overarching action exposing the information must have been undertaken knowingly. In other words, these cases require that the individual take an affirmative action with the knowledge that the information in question may be made available to a third party and/or the public at large.

3. Is CSLI Voluntarily Conveyed?

Is CSLI conveyed through an affirmative action with the knowledge that the CSLI in question may be made available to the individual's network provider? From the outset, this question teases out the problem of which level of generality to utilize. This, however, has been implicitly addressed in the Supreme Court's

353. *Id.* at 322 (White, J., dissenting).
354. *Id.* at 322–23.
355. *Id.* at 323 (quoting *Smith*, 442 U.S. at 743–44).
356. United States v. Graham, 824 F.3d 421, 430–31 (4th Cir. 2016).

prior opinions. Each opinion focused on the specific action that gave rise to the discrete piece of information in question. In *Miller*, the actions being analyzed consisted of the physical deposits at the bank.[357] In *Smith*, the Court analyzed the action of dialing a specific number.[358] In *Rooney*, it was the act of taking the trash can from the curtilage of the household to the communal trash bin.[359] Even in *Knotts* and *Karo*, the Court focused on the discrete trips and whether those occurred on public highways.[360]

The Supreme Court has implicitly instructed against taking too broad a view when analyzing voluntary conveyances. The proper analysis is not whether the individual voluntarily purchases a phone and service plan. The analysis is not even whether an individual voluntarily utilizes his or her phone during a specific timeframe. The proper analysis is to focus on the action that gives rise to the discrete CSLI data points in question.

As explained above, CSLI data points are generated at numerous times during regular activity. Most notably, they are generated when a cell phone initiates a call or other data connection, when the phone responds to a network page, and at regular time intervals as designated by the network. Each of these general categories of CSLI generation has distinct voluntary conveyance analyses.

When a cell phone attempts to initiate a call or other data connection, it contacts the network through the access channel of its current serving cell.[361] When that connection is made, the network generates a CSLI data point that indicates the type of request, the subscriber's unique identification information, and the serving cell's network address. Then the network assigns the cell phone a traffic channel for sending its data. This entire process is entirely controlled by the user of the cell phone. Therefore, the cell phone user has taken an affirmative action.

As courts have poignantly noted, one can assume that the general populace has some basic understanding that cell phones uti-

357. United States v. Miller, 425 U.S. 435, 437–39 (1976).

358. *Smith*, 442 U.S. at 741.

359. *Rooney*, 483 U.S. at 309–10, 313.

360. United States v. Karo, 468 U.S. 705, 714–16 (1984); United States v. Knotts, 460 U.S. 276, 281–85 (1983).

361. See *supra* Part I. Part I further details the technology behind cellular communication and CSLI data.

lize towers and that location has an important relation to signal strength.[362] The user has some basic knowledge that using his or her phone to initiate a call or other service makes the tower utilized available to the network provider. Accordingly, CSLI generated on account of user-initiated actions would be voluntarily conveyed and, according to the third-party doctrine, would fall outside the scope of Fourth Amendment protection.

This same concept of knowledge applies to the other two categories of CSLI generation: responding to network pages and contacting the network at regular time intervals. The cell phone user has a basic knowledge that any connection between his or her phone and the network may make the specific tower utilized available to their network provider. However, each of these two categories of CSLI generation are missing an affirmative action by the user. Cellular networks may require every phone to contact it periodically—depending on the specific network's specifications—to maintain the network's location registers.[363] This will occur regardless of any user action short of disconnecting it from the network. Further, CSLI is also generated when cell phones respond to network pages. As explained above, pages are sent to cell phones to indicate that there is incoming data, such as a call or text message.[364] Cell phones automatically respond to this page and initiate a connection in order to receive the data. Individuals may choose to ignore a call, but the phone still has to connect to the network to receive that incoming call, and that connection will still generate a discrete CSLI data point. Accordingly, neither of these categories involve an affirmative action from the user, so neither of these categories of CSLI are voluntarily conveyed to the network.

362. United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower.").

363. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 12–16 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania).

364. *See id.* at 13–14.

4. There Is a Legitimate Expectation of Privacy in CSLI Data

Under *Katz*, two questions are raised: whether the individual has "exhibited an actual (subjective) expectation of privacy and, second, [whether] the expectation [is] one that society is prepared to recognize as 'reasonable.'"[365]

There is significant evidence of a subjective expectation of privacy in historical CSLI. Eighty-two percent of American adults consider details of their physical location over time to be sensitive information.[366] As one district court noted, "[t]his figure is higher than the percentage of individuals surveyed who consider their relationship history, religious or political views, or the content of their text messages to be sensitive."[367] Approximately 19 percent of adults have turned off location tracking on their phone over concerns that a third party would be able to access it.[368] Furthermore, another 31 percent of adults were completely unaware that their cell phones were able to be tracked by any method.[369]

This subjective expectation of privacy is one that society would and does consider reasonable. There has been significant public outcry recently at the scope of NSA intelligence gathering on domestic cell phones.[370] Furthermore, in recent years states have recognized privacy expectations in CSLI. Three state high courts have struck down some form of warrantless CSLI collection on state grounds.[371] Six states passed statutes requiring search war-

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

366. PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST–SNOWDEN ERA 32 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

367. *In re* Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1024 (N.D. Cal. 2015).

368. JAN LAUREN BOYLES ET AL., PEW RESEARCH INTERNET & AM. LIFE PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES 8 (2012), http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

369. Dave Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTE PRIVACY BLOG (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.

370. John Mueller & Mark G. Stewart, *Secret Without Reason and Costly Without Accomplishment: Questioning the National Security Agency's Metadata Program*, 10 I/S J.L. & POL'Y FOR INFO. SOC'Y 407, 409 (2014).

371. Tracey v. State, 152 So.3d 504, 525–26 (Fla. 2014) (holding that the collection of active CSLI, absent a warrant, is unconstitutional); Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014) (holding that the collection of historical CSLI is uncon-

rants for historical CSLI.[372] Six more states statutorily require search warrants for active CSLI collection.[373]

Judicial unease with prolonged location tracking is also evident, along with strong evidence that society would recognize a privacy interest in CSLI as reasonable. Judges routinely question the government on the "specter of big brother" that CSLI collection conjures.[374] In *Graham*, Judge Thacker's question to the government embodied these concerns: "So, everyone in the country who has a cell phone has no reasonable expectation of privacy [in their location]?"[375] Still other judges have personal concerns, expressing obvious discomfort with the ramifications of CSLI collection on their family's privacy.[376]

B. *Charting a New Path: Balancing the Third-Party Doctrine and Digital Privacy*

CSLI embodies the difficulty of decades-old precedent in the digital age. Strict application of the third-party doctrine leads to a convoluted result, where user-generated CSLI can be obtained by court order, but non-user-generated CSLI requires a search warrant. However, to even come to this conclusion, courts must be placed outside of their proper scope and become subject-matter experts in emerging technologies. These results are anathema to coherent jurisprudence.

---

stitutional without a showing of probable cause); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (finding the warrantless collection of active CSLI to be unconstitutional on state grounds).

372. *See* COLO. REV. STAT. § 16-3-303.5(2) (2015); ME. REV. STAT. tit. 16, § 648 (2016); MINN. STAT. §§ 626A.28(3)(d), 626A.42(2) (2016); MONT. CODE ANN. § 46-5-110(1)(a) (2015); TENN. CODE ANN. § 39-13-610(b) (2016); UTAH CODE ANN. § 77–23c–102(1)(a) (LexisNexis 2015).

373. *See* 725 ILL. COMP. STAT. 168/10 (2012); IND. CODE § 35-33-5-12 (2016); MD. CODE ANN., CRIM. PROC. § 1-203.1(b)(1) (2013); VA. CODE ANN. § 19.256.2 (2015); WASH. REV. CODE 9.73.260 (2015); WIS. STAT. § 968.373(2) (2016).

374. *See* Oral Argument at 32:00–35:00, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (No. 12-12928).

375. *See* Oral Argument at 25:20, United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (No. 12-4659), http://coop.ca4.uscourts.gov/OAarchive/mp3/12-4659-20141211.mp3.

376. *Id.* at 27:48 (comments of Davis, J.) ("So a person who gets a cell phone as a gift; my step-daughter's cell phone—she's voluntarily, in other words, that's all it takes in your submission. You turn it on [and] you have voluntarily submitted to the provider's decision to keep track of your movement even for unanswered phone calls. So you literally never have to use the phone . . . ."); Oral Argument at 45:40 United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (No. 12-12928) (expressing concern that the Judge's nephew would no longer be afforded certain privacies due to using electronic devices).

It is time for the Supreme Court to accept certiorari in *Carpenter*[377] and/or *Graham*.[378] The Court has made clear it is prepared to examine the Fourth Amendment in light of new digital concerns, and this field is crying out for such treatment. CSLI collection has spawned wide-ranging confusion. Even the circuit courts have called on the Supreme Court to take action, noting that:

> [A]lthough the [Supreme] Court formulated the third-party doctrine as an *articulation* of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an *exception*. A *per se* rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy. But Justice Sotomayor also made clear that tailoring the Fourth Amendment to "the digital age" would require the Supreme Court itself to "reconsider" the third-party doctrine.[379]

The Supreme Court should re-examine the Fourth Amendment in regards to cellular location tracking capabilities and extend its rationale from *Riley*, that digital technology is subject to stronger Fourth Amendment protections than its analog counterparts. Accordingly, the Court should rule that a section 2703(d) court order is unconstitutional as-applied to the collection of CSLI and requires a search warrant under section 2703(c)(1)(A) for the collection of any CSLI.

As with the search-incident-to-arrest problem addressed in *Riley*, CSLI cases require courts to use doctrine from the 1970s that, although technically applicable, produces untenable results. Just as searching the contents of a cell phone is different than searching the pockets of somebody from the 1970s, CSLI information differs from the relatively small windows into one's life created by banking records or pen registers. Importantly, taking this approach would eliminate the need to take either of the extremes currently advocated for by opposing sides on this debate. First, it obviates the need to uphold the strict words of the third-party doctrine in spite of technological advances. Second, and perhaps more importantly, it prevents the near-complete upheaval of Fourth Amendment law in this field that some have advocated for.

---

377. Petition for Writ of Certiorari, Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016) (No. 16-402).

378. Petition for Writ of Certiorari, Graham v. United States, 824 F.3d 421 (4th Cir. 2016) (en banc) (No. 16-6308).

379. *Graham*, 824 F.3d at 437 (quoting United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring)).

Many have taken *Jones* as an opportunity to advocate for a full implementation of the mosaic theory in Fourth Amendment law.[380] However the implementation of the mosaic theory would uproot Fourth Amendment jurisprudence, cloaking much of it in doubt.[381] The mosaic theory unwisely tries to introduce an unworkable balancing test into the *Katz* analysis.[382] In the words of Professor Orin Kerr:

> The mosaic theory should be repudiated for three reasons. First, the theory raises so many novel and puzzling new questions that it would be difficult, if not impossible, to administer effectively as technology changes. Second, the mosaic theory rests on a probabilistic conception of the reasonable expectation of privacy test that is ill suited to regulate the new technologies that the mosaic theory has been created to address. And third, the theory interferes with statutory protections that better regulate surveillance practices outside of the sequential approach.[383]

By recognizing that cellular technology is fundamentally different than its analog counterpart, the Court could afford it the higher protection of a probable cause requirement without rewriting existing law. Such an approach, far from abandoning the third-party doctrine, would allow it to continue to serve its purpose outside the realm of cellular technology.

One may fairly criticize this proposition, claiming it opens the door to put other limits on the third-party doctrine. However, it is important to remember that this proposal is narrowly limited to only cellular technology and is based in its unique and ubiquitous role in modern life. Few other technological advances present similar circumstances. More importantly though, law should evolve. As time changes, so do the circumstances that the law emerged from. This recognition proves foundational to the entire concept of common law systems.

The digital age requires the third-party doctrine to evolve. Recognizing that cellular technology represents a unique and largely

380. *See generally* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012) (advocating for a statutory implementation of the mosaic theory).

381. *See* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 402–11 (2013) (detailing numerous doctrinal and conceptual concerns in implementing the mosaic theory in Fourth Amendment law).

382. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 352 (2012).

383. *Id.* at 346.

incomparable type of third-party information is the first step in modernizing the third-party doctrine. Importantly though, this step can be continuous in the Fourth Amendment's evolution as a whole. Cellular information is unprecedented in scope, but changes reflecting this basic truism do not need to be equally unprecedented in scope. There is no need to uproot the third-party doctrine or traditional Fourth Amendment search analyses; only a need to recognize that cellular technology requires reformulation of existing doctrine: CSLI collection should require a warrant.

CONCLUSION

Third-party doctrine analyses of historical CSLI leave the law in a precarious state. Non-user-generated CSLI is left protected under the Fourth Amendment, while user-generated CSLI is not. This enables law enforcement to request a section 2703(d) order under the SCA for CSLI from user-generated events. However, obtaining CSLI data from non-user-generated data is a search under the Fourth Amendment and presumptively unreasonable. Unfortunately, to date, five separate circuit courts have examined the issue of historical CSLI without examining the nuances of the technology in question. The Third Circuit held that no CSLI is voluntarily conveyed to a third party, while the Fourth, Fifth, Sixth, and Eleventh have held that all CSLI is voluntarily conveyed to a third party. None developed an understanding of the technology beyond the basic premise that using a cell phone generates CSLI in some way.

It has become necessary for the Supreme Court to accept certiorari on a historical CSLI case. The law is convoluted and outdated. A strict application of the third-party doctrine, ignoring other precedent, leads to the conclusion that only user-generated CSLI should be reachable by a section 2703(d) order. However, this is currently the law in no circuit. Furthermore, the concept that user-generated CSLI is not protected by the Fourth Amendment flouts the privacy concerns espoused in *Jones*.

Jones and *Riley* were the Court's first steps in adjusting to the digital age. It is time to take another step: to re-examine the third-party doctrine, recognizing that cellular technology presents a unique situation that was unimaginable at the third-party doctrine's origins. At its inception the third-party doctrine was appli-

cable largely by asking a common-sense question about whether an action was a voluntary conveyance. With cellular technology however, a court must develop an intimate understanding of complicated technology to accurately analyze whether an action is a voluntary conveyance.

This is not the appropriate role of courts, efficient use of judicial resources, nor is it the clear jurisprudence necessary to guide law enforcement action in accordance with the Fourth Amendment. The Supreme Court should accept and consolidate *Carpenter* and *Graham*, and establish that CSLI is unique from its third-party doctrine precedent and requires a warrant to collect.

Justin Hill *

* J.D. 2018, University of Richmond School of Law. B.A., 2014, American Military University; A.A., 2011, Defense Language Institute. I would like to extend a special thank you to Professor Clark Williams for his invaluable guidance and support. I would also like to thank my mother for giving me the strength to change; without it, I would not be here.

***