Louisiana Law Review

Volume 77 | Number 1
Louisiana Law Review - Fall 2016

Cell Phone Location Tracking: Reforming the Standard to Reflect Modern Privacy Expectations

Shannon Jaeckel

Cell Phone Location Tracking: Reforming the Standard to Reflect Modern Privacy Expectations

INTRODUCTION

If you are like most cell phone users today, chances are, your cell phone is within arm's reach of you as you read this article. Ninety-one percent of American adults own cell phones, and nearly two-thirds of that group own smartphones, which are cell phones with computer operating systems.[1] Many cell phone users are almost never without their phones during the waking day.[2] Even while sleeping, most users keep their cell phones near them and usually charge their phones on a bedside table. Immediately after waking, most cell phone users reach for their cell phones before doing anything else.[3] The International Data Corporation's ("IDC") research revealed that 63% of smartphone owners keep their phones with them for all but one hour of the day, and 79% keep their smartphones with them for all but two hours of the day.[4] The research also showed that one in four respondents could not recall a time in the day when the phones were not within reach or in the same room.[5]

As these statistics demonstrate, cell phones have transformed the way society communicates, conducts business, organizes daily affairs, and connects with others throughout the world.[6] In modern American society—a society accustomed to having the ability to be in constant contact with anyone, anytime, anywhere—the cell phone has become a

---

1. *Always Connected: How Smartphones and Social Keep Us Engaged*, INT'L DATA CORP., http://www.nu.nl/files/IDC-Facebook%20Always%20Connected%20(1).pdf [https://perma.cc/9AXV-BWRU] (last visited Oct. 13, 2015) [hereinafter *Always Connected*].

2. *See id*.

3. Research surveying American adult smartphone owners showed that within the first 15 minutes of waking up, four out of five users check their phones, and among these people 80% reach for their phones before doing anything else. *Id*.

4. *Id*. The IDC surveyed 7,446 American smartphone users between the ages of 18 and 44 over the course of one week to produce this research. *Id*.

5. *Id*.

6. *Id. See also 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. 18–19 (2010) (testimony of Prof. Matt Blaze), http://judiciary.house.gov/_files/hearings/printers/111th/111-109_57082.PDF [https://perma.cc/2JWD-ZB9B] [hereinafter *ECPA Reform*].

critical social, communication, and information tool.[7] Cell phones today are not a mere convenience; they are a basic necessity to many Americans and omnipresent in nearly all aspects of life.[8]

Society is able to stay connected because of recent developments in cellular technology, but with this convenience comes a significant drawback. Law enforcement can use cell phones to track individual's movements with greater ease. Cell phones automatically register their location with cell phone towers every seven seconds,[9] and users cannot deactivate this function while the phone is powered on.[10] Each time a cell phone connects to a cell tower, cell site location information ("CSLI") data is generated.[11] This information is capable of reconstructing a cell phone user's specific movements minute by minute.[12] Cell service providers store CSLI in cell tower records, often for several years.[13] Each year law enforcement agencies submit millions of requests to cell service providers for cell tower records, usually without a warrant.[14] To accommodate the large volume of data requests they receive, some cell service providers have created detailed handbooks describing their policies for surveillance assistance for law enforcement agents.[15] Sprint has even created a website

---

7. *Always Connected*, *supra* note 1.

8. *ECPA Reform*, *supra* note 6, at 18–19.

9. Scott A. Fraser, *Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571, 578 (2012).

10. *Cell Phone Location Tracking Public Records Request*, ACLU, https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request [https://perma.cc/2U54-JN6D] (last updated Mar. 25, 2013).

11. *See* Nathaniel Wackman, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. L. REV. 263, 269 (2015).

12. R. Craig Curtis, Michael C. Gizzi & Michael J. Kittleson, *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 75 (2014).

13. Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215, 217 (2015). According to the United States Department of Justice, Sprint keeps location tracking records for 18–24 months, and AT&T has stored cell tower records "since July 2008," suggesting they are stored indefinitely. *Cell Phone Location Tracking Public Records Request*, *supra* note 10.

14. Curtis, *supra* note 12, at 62–63.

15. Catherine Crump, *Are the Police Tracking Your Calls?*, CNN (May 22, 2012 3:23 PM), http://www.cnn.com/2012/05/22/opinion/crump-cellphone-privacy [https://perma.cc/AER8-S36Z].

for police to access the information conveniently with the simple click of a mouse.[16]

Although police commonly use these convenient practices, no uniform legal standard for judicial oversight exists.[17] The current laws governing CSLI in Louisiana and elsewhere are unclear and the laws fail to balance properly the government's interest in executing investigations with the competing privacy interests in location information. Requiring law enforcement to demonstrate probable cause that CSLI will reveal evidence of a crime and to obtain a warrant before gathering CSLI would effectively balance these interests and provide clear guidelines for law enforcement. Both the Louisiana Constitution and the Louisiana statutes governing CSLI should adopt this standard. Louisiana courts should recognize the privacy right in CSLI under Article 1, Section 5 of the Louisiana Constitution,[18] and the Louisiana legislature should enact a comprehensive statutory scheme that sets forth clear guidelines governing all areas of CSLI. Those guidelines should include exclusionary remedies and exceptions to the warrant requirement so that both the courts and law enforcement have a definitive set of rules to resolve CSLI issues.

Part I of this Comment discusses the history of CSLI technology and the relevant federal statutes. This section explains the mechanics and content of CSLI data; additionally, it illustrates recent advances in CSLI technology and the importance of this information to law enforcement. Part II analyzes the three most recent federal circuit court decisions in this area of the law. These cases identify the analytical problems surrounding CSLI and illustrate the extent to which courts have addressed these problems. Part III examines state responses to CSLI with a particular focus on how Louisiana courts and the Louisiana legislature have approached the issue in comparison with other states. Part IV proposes that the Louisiana legislature be proactive in adopting a comprehensive CSLI statutory scheme rather than waiting for federal action. Specifically, the courts should interpret the Louisiana Constitution more expansively to provide additional privacy interest protections than currently exist under

16. *Id*.
17. Curtis, *supra* note 12, at 63.
18. The Louisiana Constitution provides:

> Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search.

LA. CONST. art. I, § 5.

federal law, and the Louisiana legislature should codify this privacy interest and provide detailed guidelines. This solution is most apt to resolve the problems surrounding Louisiana for two reasons. First, it will vest a constitutionally protected interest. Second, it allows the Louisiana legislature, which is charged with adopting policies that benefit its citizenry, to adopt legislative rules that balance the government's interest in conducting effective investigations with the public's privacy interests in CSLI.

I. MODERN CELL PHONE LOCATION TRACKING

Smartphones have created more detailed and advanced CSLI.[19] Law enforcement agencies routinely utilize CSLI during investigations, and prosecutors commonly introduce CSLI as evidence in courtrooms.[20] As a result, judges and juries frequently rely on CSLI to convict criminal defendants.[21] Both the technology of CSLI and the laws controlling the government's use of CSLI illustrate why it has been an extraordinary tool to the government.

A. Cell Site Location Information and Cell Tower Technology

CTIA's Annual Wireless Industry Survey reveals that wireless subscribers in the United States used 2.88 trillion voice minutes, 9.65 trillion megabytes of data, and sent 1.89 trillion text messages in 2015.[22] Each of these connections that the wireless devices made to cell towers generated CSLI, which the cell service provider later stored. Occasionally, the government accessed CSLI without the wireless subscriber's knowledge, and in many cases without a warrant based on a showing of probable cause. The popularity of cell phones and the plethora of purposes for which they are used today create trillions of location data points each year.[23] The advancement of cellular technology coupled with the

19. *See* United States v. Graham, 796 F.3d 332, 343 n.1 (4th Cir. 2015) (explaining how smartphones communicate with the network more frequently than traditional cell phones).

20. *See, e.g.*, *Graham*, 796 F.3d at 332; *see also* State v. Marinello 49 So. 3d 488 (La. Ct. App. 2010).

21. *See, e.g.*, *Undisclosed: The State vs. Adnan Syed: Ping*, PARTNERS IN CRIME MEDIA (July 27, 2015) (downloaded using iTunes).

22. *Annual Wireless Industry Survey*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey [https://perma.cc/7HPT-BYB6] (last updated May 2016).

23. *See id*.

proliferation of cell sites has led to voluminous, detailed, and precise cell tower records that the government has used to its advantage in both investigative and prosecutorial contexts.

1. The Mechanics of CSLI

To function, a cell phone constantly connects to a cellular network by communicating with cell sites in its immediate area.[24] These communications occur when the phone sends or receives a call or text message.[25] Smartphones generate more frequent communications with the network through applications installed on the phone.[26] For example, each time the smartphone updates an email inbox,[27] shares pictures on social media, or provides navigation data, the smartphone connects to the network.[28] Cell sites, or cell towers, are radio base stations that cellular service providers maintain throughout their geographic coverage areas.[29] A registration process determines the particular cell site responsible for connecting the cell phone to the network.[30] As a cell phone moves throughout the coverage area, it will periodically identify itself to cell towers within its vicinity.[31] Once the cell phone has located nearby cell towers, the phone ranks these towers according to the strength of the signal[32] and registers with the cell tower best equipped to process a call through its radio signal's strength.[33] The registration process occurs continuously and automatically while the phone is turned on.[34] When a phone moves away from the originating cell site during a call, the call is "handed off" to a new tower.[35] When a cell

24. *See Electronic Communications Privacy Act Reform: Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 40 (2010) (statement of Prof. Orin Kerr), http://judiciary.house.gov/_files/hearings/printers/111th/111-98_56271.PDF [https://perma.cc/AR46-7MY8]; *Graham*, 796 F.3d at 343; *ECPA Reform*, *supra* note 6, at 20.

25. *Graham*, 796 F.3d at 343; *ECPA Reform*, *supra* note 6, at 20.

26. *Graham*, 796 F.3d at 343 n.1.

27. *Id*.

28. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (April 1, 2015) http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ [https://perma.cc/NVE4-B49R].

29. *ECPA Reform*, *supra* note 6, at 20.

30. *See* Fraser, *supra* note 9, at 578.

31. *See ECPA Reform*, *supra* note 6, at 20.

32. Fraser, *supra* note 9, at 578.

33. *ECPA Reform*, *supra* note 6, at 13.

34. Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT L.J. 421, 426 (2007).

35. *ECPA Reform*, *supra* note 6, at 20; *Undisclosed*, *supra* note 21.

phone is turned on and moving throughout the network, the cell service provider tracks the tower with which the phone is registered.[36] Cell phone companies record this information in cell tower records for a variety of business purposes.[37]

Cell tower records contain detailed information such as the date and time of calls made or received, the phone numbers called, the duration of each call, and the cell towers that began and ended the call.[38] The amount of information that each cell service provider stores varies depending on a cell service provider's technology and business decisions about data retention.[39] Although some cell service providers limit cell tower record information to the data created during the beginning and the end of a call, other providers store all of the data, including location information collected during a call and when the phone is idle.[40] The length of time that cell service providers store CSLI also varies.[41] An increasing number of cell service providers are opting to maintain more detailed cell tower records.[42] The trend toward detailed cell tower records will likely continue because once a cell tower is installed, the cost of collecting and storing detailed, frequently updated cell tower records is relatively low.[43]

---

36. *ECPA Reform*, *supra* note 6, at 14.

37. *Reforming the Electronic Communications Privacy Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 2 (2015) (Statement of Elana Tyrangiel, Principal Deputy Assistant Att'y Gen.), http://www.judiciary.senate.gov/imo/media /doc/09-16-15%20Tyrangiel%20Testimony.pdf [https://perma.cc/3EPC-4HRL] [hereinafter *Reforming the ECPA*]. Some of the business purposes that CSLI serves include establishing a communications channel, routing a communication to its intended destination, and billing customers for communications services. *Id*.

38. Mark Hansen, *Prosecutors' Use of Mobile Phone Tracking is 'Junk Science,' Critics Say*, AM. B. ASSOC. J. (June 1, 2013, 8:50 AM), http://www.abajournal.com/magazine/article/prosecutors_use_of_mobile_phone_tracking_is_junk_science_critics_say/ [https://perma.cc/7EXQ-KD42].

39. Fraser, *supra* note 9, at 579.

40. *See id*. at 580; *see also ECPA Reform*, *supra* note 6, at 27–28.

41. According to the United States Department of Justice, Sprint keeps location tracking records for 18 to 24 months, and AT&T has stored cell tower records "since July 2008," which suggests that they are stored indefinitely. *Cell Phone Location Tracking Public Records Request*, *supra* note 10.

42. *ECPA Reform*, *supra* note 6, at 27–28. Maintaining high resolution CSLI about each customer is a cost efficient way for cell service providers to collect highly valuable information for network management, marketing, and developing new services. *Id*.

43. *Id*.

Cell service providers are also continually building new cell towers to accommodate the explosive consumer demand for cellular service.[44] As the number of cell towers steadily increases, the geographic area served by each cell tower decreases.[45] Several years ago CSLI could provide only a vague picture of a person's location.[46] Presently, however, smaller cell coverage areas allow for collection of more precise location information.[47] Although some of the largest cell coverage areas in rural locales can still be several miles in diameter, modern technology provides much more specific locations, such as a floor or individual room in a building or private home.[48]

2. The Use of CSLI by Law Enforcement

As cell service providers deploy more advanced location technologies, law enforcement will receive more precise and more valuable CSLI.[49] Law enforcement commonly uses this information to track individuals.[50] Additionally, although law enforcement commonly obtains cell phone records about a particular person, law enforcement sometimes requests data for all phones connected to a particular tower at a particular time.[51] In response to a record request that the American Civil Liberties Union submitted to state and local law enforcement agencies throughout the country regarding cell phone tracking, approximately 250 police departments responded with 2,700 pages of documents.[52] The responses

44. *Id*. at 19. The number of cell sites in the United States has increased from 162,986 in December 2003 to 298,055 in December 2014. *Annual Wireless Industry Survey*, *supra* note 22.

45. *ECPA Reform*, *supra* note 6, at 25.

46. Wackman, *supra* note 11, at 271.

47. *See id*.

48. *ECPA Reform*, *supra* note 6, at 15–16.

49. *See id*. at 29.

50. *See Cell Phone Location Tracking Public Records Request*, *supra* note 10.

51. *Id*. The investigation of the Boston Marathon bombing provides an example of this practice. Using processes outlined in the Electronic Communications Privacy Act, FBI agents requested all CSLI generated for calls and texts terminated at the bombsite around the time that the bombs were detonated. *Reforming the ECPA*, *supra* note 37, at 3. These cell tower records later proved to be critical during the investigation to help identify the bombers and their associates. *Id*. Some of the cell tower records were used at trial to show the communications between the bombers at critical times. *Id*.

52. *See Cell Phone Location Tracking Public Records Request*, *supra* note 10.

revealed that although almost all of the police departments track cell phones, very few reported consistently obtaining warrants.[53]

CSLI provides law enforcement with a priceless investigative tool because many law enforcement agencies located in areas employing advanced cellular technologies are able to calculate cell phone users' locations with a precision that approaches that of a GPS.[54] In fact, CSLI is often more useful to law enforcement than even traditional GPS devices for several reasons.[55] First, CSLI yields some of the same results as physical surveillance, but CSLI obviates purchasing GPS devices and paying police officers for their time spent installing and subsequently removing GPS devices. Thus, police departments that lack the resources for extended GPS surveillance benefit from CSLI.[56] Second, the cellular network produces CSLI without any indication to individuals that they are being tracked,[57] whereas GPS devices, if discovered by the individual being tracked, would alert the individual to surveillance efforts. Lastly, CSLI allows law enforcement to track individuals in areas inaccessible to GPS devices without a warrant because of their constitutionally protected status, such as inside a home.[58] Because cell phones have become such a ubiquitous part of modern American life, cell phones accompany their users everywhere,[59] resulting in virtually constant surveillance in both private and public spaces.[60] GPS devices, on the other hand, attach to specific areas or items, such as a car or container, that do not remain with

---

53. *Id*.

54. *ECPA Reform*, *supra* note 6, at 23; M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007). A Global Positioning System ("GPS") processes signals broadcasted by satellites orbiting the earth to mathematically determine the location of the GPS device and permits continuous, precise tracking of an individual's movements. April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting* Knotts *and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 662, 665 (2005).

55. *ECPA Reform*, *supra* note 6, at 30.

56. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 408 (1997).

57. *Id*.

58. *ECPA Reform*, *supra* note 6, at 30.

59. State v. Earls, 70 A.3d 630, 643 (N.J. 2013) ("[C]ell-phone use has become an indispensable part of modern life. The hundreds of millions of wireless devices in use each day can often be found near their owners—at work, school, or home, and at events and gatherings of all types.").

60. *Graham*, 796 F.3d at 348.

individuals as continuously as a cell phone does, thus limiting the availability of location information collected by the GPS devices.[61]

Examination of cell tower records not only helps law enforcement officials locate suspects,[62] but also reveals with whom a suspect communicates, at what time, and for how long.[63] Officers gather CSLI early in investigations and use it to generate at least part of the probable cause justification necessary for subsequent search and arrest warrants.[64]

In the past several years, location data has provided law enforcement with not only investigatory but also prosecutorial value.[65] Lawyers can use CSLI to achieve many evidentiary objectives during trial, including destroying a suspect's alibi and establishing presence near a crime scene at the approximate time of the crime.[66] Because establishing a defendant's location during the crime is often one of the most important factors to a jury, prosecutors supplement traditional defendant location evidence, such as eyewitness testimony and physical evidence, with cell site analysis from CSLI to connect defendants with places relevant to the charged offense.[67] Prosecutors use inferences from even fairly imprecise CSLI as key evidence to enhance the value of the data in the jury's eyes.[68]

---

61. *See id*.

62. An example of law enforcement using CSLI to locate a suspect is the shooting of a police lieutenant in Baton Rouge, Louisiana. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 4 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen.), http://www.judiciary.senate.gov/imo/media/doc/11-4-6%20Baker%20Testimony.pdf [https://perma.cc/QP38-QS83]. While attempting to stop the suspect, the suspect shot the lieutenant in the neck and fled the scene. *Id*. After investigation, the suspect was identified and an arrest warrant was obtained for attempted first-degree murder of a police officer. *Id*. In their efforts to locate and arrest the suspect, the officers obtained court orders compelling the suspect's cell phone company to provide cell tower records. *Id*. The CSLI ultimately allowed officers to confirm the suspect's location. *Id*.

63. Fraser, *supra* note 9, at 582.

64. *See Cell Phone Location Tracking Public Records Request*, *supra* note 10, at 2.

65. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 725 (2011).

66. Wackman, *supra* note 11, at 267.

67. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATTYS' BULL. 6, 16 (2011), http://www.justice.gov/sites/default/files/usao/legacy/2011/11/30/usab5906.pdf [https://perma.cc/8P2K-SS2V].

68. Freiwald, *supra* note 65, at 725–26.

One example of a prosecutor relying heavily on unreliable CSLI to convict a defendant comes from *State v. Adnan Syed*.[69] In 2000, Syed was convicted and sentenced to life imprisonment for killing his ex-girlfriend.[70] The state used cell tower data to link Syed to Leakin Park, where the body was found.[71] The prosecution had no physical evidence or eyewitnesses tying Syed to the murder.[72] The only non-CSLI evidence that the prosecution presented was the testimony of a friend, Jay Wilds,[73] which was also unreliable because Wilds changed his story to match the cell tower records after the police confronted him with the records.[74] Although either piece of evidence alone would not likely have been sufficient to prove Syed's guilt beyond a reasonable doubt, the prosecutors aggressively and successfully asserted that the cell tower records corroborated Wilds's story.[75] The CSLI available during Syed's trial was far less precise than the CSLI available today, but it was sufficient to convince the jury of Syed's guilt beyond a reasonable doubt. The precision of CSLI and the frequency of cell phone use today as compared to in 2000 has changed drastically, and as a result, so has the need for protection of privacy interests in location information.

B. Electronic Communications Privacy Act

Congress passed the Electronic Communications Privacy Act ("ECPA") in 1986 to expand and revise federal wiretapping and electronic eavesdropping laws.[76] Congress sought not only to "create a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement," but also to "support the creation of new technologies by assuring consumers that their personal information would remain

---

69. *See generally Undisclosed*, *supra* note 21.

70. Justin Fenton, *Adnan Syed's Defense Attorney Says He Has New Evidence to Overturn Conviction*, BALTIMORE SUN (Aug. 24, 2015, 7:27 PM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-syed-cell-phone-motion-20150824-story.html [https://perma.cc/B4XF-H725].

71. *Id.*; *see also Undisclosed*, *supra* note 21.

72. Fenton, *supra* note 70.

73. *Id*.

74. *Undisclosed*, *supra* note 21.

75. *Id*. For further discussion of the cell phone data controversy that the podcasts *Undisclosed: The State vs. Adnan Syed* and season one of *Serial* reveal, *see The Legal Ease: Ep. 6 Hon James Dennis: Personal History Part 2*, LA. L. REV. (Feb. 21, 2016) (downloaded using iTunes).

76. *Electronic Communications Privacy Act (ECPA)*, EPIC.ORG, https://epic.org/privacy/ecpa/ [https://perma.cc/66UJ-9EK5] (last visited Sept. 30, 2015).

safe."[77] The ECPA consists of several sets of laws governing the collection and disclosure of both content and non-content information related to electronic communications,[78] including the Pen Register Statute[79] controlling real-time CSLI and the Stored Communications Act ("SCA")[80] controlling historical CSLI. The ECPA was originally enacted during a considerably different technological era.[81] Although Congress has updated the ECPA several times, the statute—particularly the SCA provisions controlling disclosure of cell tower records—has failed to keep pace with changes in cellular technology and the way it is used.[82]

The primary statute that governs the disclosure of historical CSLI is the SCA.[83] Historical CSLI reveals data generated during past cell phone connections to cell towers.[84] Barring subscriber consent, the statute requires the government to obtain a warrant or a court order before compelling disclosure of historical CSLI.[85] A warrant authorizing disclosure requires an impartial magistrate to find probable cause.[86] Section 2703(d) mandates that a court of competent jurisdiction issue a court order for disclosure "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought are relevant and material to an ongoing criminal investigation."[87] The Section 2703(d) standard requiring specific

77. *Id*.

78. CSLI is generally considered to be non-content information because it involves the numbers used to make calls, the duration of calls, and which cell towers were used to make those calls, rather than the actual words communicated through the call. Corbett, *supra* note 13, at 218. Therefore, content-based electronic communications are outside the scope of this article.

79. 18 U.S.C. §§ 3121–3127 (2012).

80. 18 U.S.C. §§ 2701–2712 (2012).

81. *Reforming the ECPA*, *supra* note 37, at 4.

82. *Id*.

83. 18 U.S.C. § 2703 (2012).

84. Corbett, *supra* note 13.

85. 18 U.S.C. § 2703(c) (2012).

86. FED. R. CRIM. P. 41(d). The warrant requirements in the Federal Rules of Criminal Procedure are consistent with the Fourth Amendment. *See* U.S. CONST. amend. IV:

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

87. 18 U.S.C. § 2703(d) (2012).

and articulable facts is essentially a reasonable suspicion standard.[88] The probable cause standard for securing a warrant is substantially higher than the specific and articulable facts standard required for a Section 2703 court order.[89] Although the probable cause standard requires that the information sought be evidence of a crime,[90] the Section 2703(d) standard allows the government to seek any information that is materially relevant to an ongoing investigation.[91] The Section 2703(d) standard thus permits acquisition of CSLI that will yield not necessarily evidence of a crime but rather information that will somehow aid in the investigation of a crime,[92] which permits broader inquiries into a wider range of targets.[93]

Despite the significant disparities in the level of proof required for a warrant versus a Section 2703(d) order, Section 2703 offers no express direction about when the government should seek a warrant as opposed to an order.[94] Although the sealed nature of the government's requests makes knowing the full scope of such inquiries impossible, the lesser standard and anecdotal evidence suggest that the Section 2703(d) standard has facilitated much more information gathering than the probable cause standard would permit.[95] The statute's lack of clear guidance has sparked much debate over the proper standard of proof required to obtain CSLI under the SCA.

Real-time CSLI is governed by 18 U.S.C. Section 3122, commonly known as the Pen Register or Trap and Trace Statute.[96] Real-time CSLI shows cell phone connections to cell towers as they actually occur.[97] The Pen Register statute also requires the government to obtain a court order before compelling disclosure of cell tower data. A Section 3122 court

88. United States v. Graham, 796 F.3d at 343–44 (quoting In Re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013)).

89. *Id.* at 344.

90. *See* FED. R. CRIM. P. 41(c); *see also* In re Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (noting the difference in the standards because probable cause requires a finding that the information sought is itself evidence of a crime rather than relevant and material to the investigation).

91. 18 U.S.C. § 2703(d) (2012).

92. Freiwald, *supra* note 65, at 697–98.

93. *Id*.

94. *Graham*, 796 F.3d at 343–44 (citations omitted) (quoting In Re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013)).

95. Freiwald, *supra* note 65, at 697–98.

96. Corbett, *supra* note 13, at 218.

97. *Id*. at 217.

order requires a "certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[98] Thus, the standard for a Section 3122 court order is even lower than the Section 2703(d) standard in that, unlike the Section 2703(d) order, the applicant need not demonstrate specific and articulable facts demonstrating the real-time CSLI's relevance to the investigation.

The ECPA does not achieve the goals Congress intended in balancing the interest of the government in prosecution with the interest of the public in privacy. Both Section 2703(d) and Section 3122 provide the government with open avenues to obtain CSLI without a showing of probable cause and, thus, do not have restrictions necessary to prevent violations of privacy. Although the ECPA serves the needs of law enforcement by allowing almost unfettered access to CSLI during investigations, the ECPA fails to strike an appropriate balance between the needs of law enforcement and the privacy interests of citizens. The significant inequities in this balancing equation have given rise to litigation that has sharply divided courts throughout the country.[99]

II. THE CELLULAR CIRCUIT BOARD SPLIT

Advances in cellular technology have forced courts to reconsider whether to follow the legal standards that governed individual privacy rights during a much earlier time or to alter them in light of the newest and most prevalent method of search—CSLI tracking.[100] Current Supreme Court jurisprudence governing the search doctrine fails to consider new cellular technologies and thus does not provide guidance to lower courts.[101] The United States courts of appeals, faced with the issue of what standard of proof should apply to obtain CSLI, have attempted to reconcile the rapidly evolving technological landscape with unsettled, 30-year-old Fourth Amendment precedent.[102] Although each court has framed the issue by reference to the overarching question of whether individuals have a

98. 18 U.S.C. § 3122(b)(2) (2012).

99. *See, e.g.*, United States v. Davis, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015); *see also Graham*, 796 F.3d at 332.

100. *Fourth Amendment – Warrantless Searches – New Jersey Supreme Court Holds That State Constitution Requires Police to Obtain Warrant Before Accessing Cell-Site Location Information.* – State v. Earls, 70 A.3d 630 (N.J. 2013), 127 HARV. L. REV. 2164, 2164 (2014).

101. *Id*.

102. Wackman, *supra* note 11, at 293.

legitimate privacy interest in location information, the courts' differing conclusions have created a federal circuit split.

A. Inside the Circuit Board: Fourth Amendment Precedent Controlling the Inquiry

The CSLI analysis implicates multiple strands of Fourth Amendment jurisprudence and courts have generally used two constitutional approaches—the third-party doctrine and the analogy to GPS tracking cases.[103] Some courts use the third-party doctrine to justify government access to CSLI without a warrant.[104] Other courts have focused on drawing comparisons to GPS tracking cases when formulating a stricter Fourth Amendment rationale to strike down government access to CSLI.[105]

The two-pronged test established by *Katz v. United States* answers the overarching question of whether citizens have a privacy interest in their CSLI.[106] In *Katz*, the Supreme Court held that the attachment of an eavesdropping device to a public phone booth, which recorded the defendant's conversation, was a search under the Fourth Amendment.[107] Justice Harlan's concurrence set forth the operative test used to answer the question of whether an activity constitutes a search within the meaning of the Fourth Amendment.[108] First, a person must have "exhibited an actual (subjective) expectation of privacy" and, second, that expectation must be one that "society is prepared to recognize as reasonable."[109] The *Katz* reasonable expectation of privacy test has been influential: it determined

---

103. *Id.* at 318. *See generally* United States v. Jones, 132 S. Ct. 945 (2012); Smith v. Maryland, 442 U.S. 735 (1979); Katz v. United States, 389 U.S. 347 (1967); United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984); Kyllo v. United States, 533 U.S. 27 (2001). *See also* Wackmam, *supra* note 11, at 318.

104. *See, e.g.*, In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013) (quoting *Jones*, 132 S. Ct. at 961 (Alito, J., concurring in the judgment)) (explaining that the third party doctrine applies to CSLI because the government asks cell service providers to turn over records that the provider has already created using CSLI collected); *see also* United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015) ("The longstanding third-party doctrine plainly controls the disposition of this case.").

105. *See, e.g.*, United States v. Graham, 796 F.3d 332, 346–47 (comparing examination of historical CSLI to the GPS monitoring in *Karo* and *Kyllo*).

106. *See Katz*, 389 U.S. 347 (1967).

107. *Id*. at 353.

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

109. *Id*.

the outcome of landmark Supreme Court cases involving assisted surveillance and continues to guide Fourth Amendment search inquiries today.[110]

1. The Third-Party Doctrine

The federal circuits have reached different conclusions about whether the third-party doctrine, established in *Smith v. Maryland*,[111] is applicable to CSLI.[112] In *Smith*, law enforcement used a pen register device without a warrant to record phone numbers dialed by the suspect's private phone.[113] The Court held that no legitimate privacy expectation or Fourth Amendment protection existed in the record of phone numbers that a person dials.[114] The Court reasoned that because the caller voluntarily provides the phone numbers dialed to the phone company, which keeps record of phone numbers in its normal course of business, the caller could claim no legitimate privacy expectation in that information.[115] Thus, under the third-party doctrine, an individual maintains no legitimate expectation of privacy in information that is voluntary disclosed to third parties.[116]

Since *Smith* in 1979, however, technological advancements have raised doubts as to whether the third-party doctrine remains applicable. In *United States v. Jones*, the Court held that installation of a GPS device on a suspect's car constituted a search under the Fourth Amendment and required probable cause and a warrant.[117] Although the majority opinion

110. *See, e.g.*, United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015) (analyzing Davis's privacy interest in his CSLI under the *Katz* reasonable expectation of privacy test); *see also Graham*, 796 F.3d at 345 (holding that cell phone users have both a subjective and objective reasonable expectation of privacy in CSLI).

111. 442 U.S. 735 (1979).

112. *Compare* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013) (quoting United States v. Jones, 132 S. Ct. 945, 961 (2012) (Alito, J., concurring in the judgment)) (explaining that the third-party doctrine applies to CSLI because the government is asking cell service providers to produce records the provider has already created), *and Davis*, 785 F.3d at 512 ("The longstanding third-party doctrine plainly controls the disposition of this case."), *with Graham*, 796 F.3d at 353 ("It is clear to us . . . that cell phone users do not voluntarily convey their CSLI to their service providers. The third-party doctrine . . . is therefore inapplicable here.").

113. *Smith*, 442 U.S. at 737.

114. *Id*. at 745–46.

115. *Id*.

116. *Id*. at 743–44.

117. 132 S. Ct. 945, 949 (2012).

relied primarily on the notion of trespass, Justice Sotomayor's concurring opinion focused on reasonable expectations of privacy.[118] She noted that the third-party doctrine was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[119]

Justice Sotomayor also reasoned that a trespass analysis is not applicable in surveillance situations that involve the mere transmission of electronic signals.[120] Instead, she emphasized the importance of reasonable expectations of privacy and how technological evolutions shape societal expectations.[121] Justice Sotomayor analyzed particular attributes of GPS technology that are relevant to the *Katz* analysis, such as the ability of GPS to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[122] Justice Sotomayor also expressed concerns about the government's ability to collect substantial amounts of private information about individuals at a low cost and with minimal restraints, which leads to police abuse.[123]

This observation is particularly applicable in the CSLI context because in the past, the substantial government time and resource expenditures required for extensive tracking and monitoring operated as a check on abusive law enforcement practices. With the ease of electronic tracking and monitoring, however, these checks no longer exist.[124] As Justice Sotomayor suggested, when applying the *Katz* analysis to electronic surveillance methods such as CSLI tracking, the more central Fourth Amendment issue should be "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[125] Modern society expects these types of details to remain private, regardless of how or whether the information revealing these intimate details ultimately comes into a third party's

---

118. *Id*. at 955.

119. *Id*. at 957 (Sotomayor, J., concurring). Justice Sotomayor refused the assumption that all of the information "voluntarily disclosed to some member of the public for a limited purpose" while carrying out their everyday tasks is "for that reason alone, disentitled to Fourth Amendment protection." *Id*.

120. *See id*. at 955.

121. *Id*.

122. *Id*.

123. *Id*. at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

124. Tracey v. State, 152 So.3d 504 (Fla. 2014).

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

possession.[126] Thus, the *Katz* reasonable expectation of privacy test might be the more appropriate doctrine to apply to CSLI because it is more suited for adaption to advancements in technology.

2. The GPS Tracking Trilogy: Knotts, Karo, and Kyllo

Three relevant Supreme Court cases involving technological surveillance further inform the CSLI inquiry: *U.S. v. Knotts*,[127] *U.S. v. Karo*, [128] and *Kyllo v. U.S.*[129] *Knotts* and *Karo* involved the installation of beepers inside chemical containers to track the defendants' locations.[130] In *Knotts*, the police used the beeper to follow the defendant on public roads to a remote cabin.[131] The Court held that because the beeper simply enhanced law enforcement's ability to follow the car while it was on public roads, where anyone can observe an individual, the defendant had no reasonable expectation of privacy in his location on public streets.[132] In *Karo*, the Court held that the monitoring of the beeper while the container was inside Karo's private residence, where an individual does have a legitimate privacy expectation, would be a Fourth Amendment violation absent a warrant based on probable cause.[133] The Court further explained that using an electronic device without a warrant to infer facts that visual surveillance could not reveal, such as whether a particular item is located inside a private residence or to confirm later that the item remains inside the residence, is an unreasonable search under the Fourth Amendment absent a warrant.[134] The Court ruled that this type of location tracking "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, regardless of whether the tracking reveals information directly or through inference.[135]

In *Kyllo*, the government used a thermal imaging device, classified as a tracking device, to determine whether the home was emitting a high level of heat, which is indicative of indoor marijuana cultivation.[136] The

126. United States v. Graham, 796 F.3d 332, 357 (4th Cir. 2015).
127. 460 U.S. 276 (1983).
128. 468 U.S. 705 (1984).
129. 533 U.S. 27 (2001).
130. *See generally Knotts*, 460 U.S. 276, *and Karo*, 468 U.S. 705.
131. *Knotts*, 460 U.S. at 278.
132. *Id*. at 285.
133. *Karo*, 468 U.S. at 716.
134. *Id*. at 714–15.
135. *Id*. at 707.
136. *Kyllo*, 533 U.S. at 29–30.

government then obtained a warrant based on the information they gathered from the thermal imagining device, which led to the discovery of a marijuana-growing operation inside the suspect's house.[137] Finding that the home is entitled to privacy protections, the Court held that when the government discovers details about the home's inside that are unknowable via traditional visual surveillance through a device not in general public use, a Fourth Amendment search has occurred.[138] The device did not reveal any private activities occurring inside the home, but this fact was unimportant to the Court's determination because the Fourth Amendment's protection of the home is not related to the quality or quantity of information discovered.[139] The Court reasoned that limiting the prohibition on thermal imaging devices to only intimate details would result in an impractical and unworkable test.[140] Thus, the Court held that the details discovered were intimate because they revealed information about the activities inside the home, therefore entitling such information to Fourth Amendment protection from unreasonable searches.[141] Although none of the Fourth Amendment jurisprudence speaks directly to the issue of CSLI, courts have analogized the attributes of CSLI tracking to GPS monitoring. Because CSLI arguably shares some of the same attributes as a GPS device but simultaneously serves as third-party record, the conclusions that the courts have reached vary.

B. The Fifth Circuit's Approach

In *In Re Application of the United States for Historical Cell Site Data*, federal authorities submitted a Section 2703(d) court order for CSLI in connection with three separate criminal investigations.[142] The magistrate judge denied the request and held that historical CSLI required a warrant.[143] The district court agreed.[144] On appeal, the United States Court of Appeals for the Fifth Circuit applied the third-party doctrine, holding that CSLI is "clearly a business record" because "the cell service provider collects and stores historical cell site data for its own business purposes."[145] The court assumed not only that cell phone users understand that the mere use of a cell phone conveys location information to a service

137. *Id*.
138. *Id*. at 40.
139. *Id*. at 37.
140. *Id*. at 38.
141. *Id*.
142. 724 F.3d 600, 602 (5th Cir. 2013).
143. *Id*.
144. *See id*. at 602–03.
145. *Id*. at 611–12.

provider, but also that they are aware that cell service providers retain this information and give it to law enforcement upon request.[146] The court relied on cell phone users' understanding that cell phones must send signals to cell towers to connect calls in support of its assumption that cell phone users necessarily know that location information is conveyed.[147] Lastly, the court stated that even if cell-phone-to-tower signal transmission was not common knowledge, the contractual terms of service and privacy policies notify users that a provider collects this information and will release these records to government officials if the provider receives a court order.[148]

The Fifth Circuit drew several assumptions regarding the extent of cell phone user awareness relating to CSLI practices.[149] A recent study that the Federal Trade Commission conducted, however, appears to contradict directly the assumptions upon which the Fifth Circuit relied in reaching its holding.[150] The study revealed that most consumers are unaware of the extent of the data collection and storage occurring on their mobile devices.[151] The study further revealed that when researchers alerted consumers to these practices, "consumers are typically surprised and view these practices as underhanded."[152] Studies have also shown that cell phone users often do not read or understand their providers' privacy policies.[153] Therefore, these research findings, which raise doubts about whether the public knows or has even considered cell phone providers' practices,[154] are inconsistent with the assumptions that the Fifth Circuit drew.

---

146. *Id*. at 614.

147. *Id*. at 613.

148. *Id*.

149. *See id*. at 613–14.

150. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY: A FEDERAL TRADE COMMISSION STAFF REPORT (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/CJD9-M3SN].

151. *Id.* at 10.

152. *Id*.

153. *Id*.; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y INFO. SOC'Y 543, 544 (2008).

154. *See* Megan L. McKeown, *Whose Line Is It Anyway? Probable Cause and Historical Cell Site Data*, 90 NOTRE DAME L. REV. 2039, 2050–51 (2015).

C. The Eleventh Circuit's Approach

United States v. Davis involved an investigation of several armed robberies over a two-month period.[155] After Davis's arrest, the government applied to a federal magistrate judge for a Section 2703(d) court order.[156] The magistrate judge's order granted the request and the cell service provider complied.[157] The prosecution later used the information gathered under the authority of this court order to argue that Davis was near the robbery locations when the robberies occurred.[158] On rehearing, the en banc panel held that the Section 2703(d) court order did not violate the Fourth Amendment because Davis had no reasonable expectation of privacy in the cell tower records.[159] Adopting the Fifth Circuit's reasoning, the court concluded that the third-party doctrine controlled the disposition of the case.[160] The court applied the *Katz* reasonable expectation of privacy test and held that even if Davis had a subjective expectation of privacy, the expectation was objectively unreasonable because there is no evidence that cell phone users are unaware of the functions of cell towers or the recordation of cell tower usage.[161]

Noting the limited nature of Davis's CSLI,[162] the court stated that Davis's CSLI was too imprecise to paint a detailed, accurate picture of his personal activities.[163] Notably, however, the cell phone technology used in *Davis* was significantly older and less advanced than today's technology.[164] Thus, whether the court would have reached the same result if the technology used in *Davis* were capable of generating more comprehensive and precise CSLI is questionable. The *Davis* court noted that Davis used an older cell phone, which provided no real-time tracking, no location data associated with his text messages, and no Wi-Fi-based location surveillance,[165] even in the relatively urban area of South Florida.[166] Had Davis been using the cellular technology that the majority of cell phone

155. United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015).
156. *Id*. at 502.
157. *Id*.
158. *Id*. at 501–02.
159. *Id*. at 511.
160. *Id*. at 512.
161. *Id*. at 511.
162. *See id*. at 503.
163. *Id*. at 515.
164. *See id*. at 503.
165. *Id.* at 503.
166. *See id*. at 500.

users currently use—a smartphone—the CSLI released to law enforcement would likely have conveyed significantly more details of Davis's personal life. Some commentators have suggested that in light of this distinction, the *Davis* ruling should not be read as justifying cell phone location tracking; rather, the ruling delayed the resolution of the question.[167] Because the Eleventh Circuit decided *Davis* in 2015, the holding's failure to consider law enforcement's current utilization of CSLI is surprising. As a result, the *Davis* decision looks backward rather than forward because it applies to monitoring that is several years old—before new technology such as smartphones allowed for collection of more detailed and precise CSLI.[168]

D. The Fourth Circuit's Approach

In *United States v. Graham*, two defendants were charged for a series of armed robberies in Baltimore, Maryland.[169] The police obtained two Section 2703(d) court orders directing cell service providers to disclose 221 days of historical CSLI.[170] The cell service providers complied with the order, revealing 29,659 location data points for defendant Graham and 28,410 for his co-defendant Jordan.[171] Unlike the Fifth and Eleventh Circuits, the United States Fourth Circuit held that the government's warrantless procurement of CSLI amounted to an unreasonable search in violation of the Fourth Amendment.[172] The court classified this practice as a Fourth Amendment search because examination of a person's CSLI enables the government to track the movements of a cell phone and thus its user across public and private spaces and to discover the user's private activities and personal habits.[173] In reaching this conclusion, the court referenced both the third-party doctrine and the GPS tracking cases.

The court analogized examination of historical CSLI to GPS tracking, reasoning that like the searches in *Karo* and *Kyllo*, CSLI allows the government to place individuals and their personal property—their cell phones—at their homes and other private locations at specific points in time.[174] The court emphasized that unlike the single instances in *Karo* and

---

167. Andy Greenberg, *Court's Reversal Leaves Phones Open to Warrantless Tracking*, WIRED (May 5, 2015, 5:37 PM), http://www.wired.com/2015/05/courts-reversal-leaves-phones-open-warrantless-tracking/ [https://perma.cc/E3E4-PRDG].

168. *Id*.

169. United States v. Graham, 796 F.3d 332, 338 (4th Cir. 2015).

170. *Id*. at 344.

171. *Id*. at 350.

172. *Id*. at 338.

173. *Id*. at 345.

174. *Id*. at 346–47.

Kyllo, 221 days of CSLI could likely place each defendant at home on not one, but several occasions.[175] The court further explained that the Supreme Court in *Karo* and *Kyllo* recognized the location of individuals and their property within a particular time as "critical" private details protected from the government's intrusive use of technology.[176]

Although extended CSLI monitoring is likely to place an individual in private locations on various occasions, this scenario does not always occur. For instance, if a cell phone is turned off or makes few or no connections to the network, the likelihood of private details being revealed is lower. Recognizing this possibility, the court emphasized that "the government cannot know in advance of obtaining CSLI exactly how revealing it will be or whether it will detail the cell phone user's movements in private spaces."[177] The Fourth Circuit also rejected the district court's assertion that CSLI is insufficiently precise in identifying locations to invade a reasonable privacy expectation.[178] The court stressed that cell service providers are improving their networks by installing lower-power cell towers that are capable of covering areas as small as 40 feet,[179] and when analyzing issues involving CSLI, courts must take such technological developments into account.[180]

The *Graham* court adopted a forward-looking approach that considers the increasing precision that CSLI continues to provide. Decisions in which holdings are limited to only the specific facts and technology before the court are less able to account for the current state of CSLI tracking, which is detailed, easily accessible to law enforcement, and increasingly precise.[181] By recognizing the intense competition among cell service providers and the likelihood of continuing use of small cells, the Fourth

175. *Id*.
176. *Id*.
177. *Id*. at 349–50.
178. *Id*. at 350.
179. *Id*. at 350–51.
180. *Id*.
181. *See, e.g.*, In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (recognizing the rapidly evolving technological landscape, the court limited its holding to only historical CSLI for specified cell phones at the points at which the user places and terminates a call and declined to extend its holding to requests for CSLI for the duration of calls or for when the phone is idle); United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015) (noting that the CSLI at issue was generated not continuously, but rather only when Davis was making or receiving calls).

Circuit provides an accurate analysis of the effects of warrantless CSLI collection on individuals today.[182]

Finding that cell phone users do not convey their CSLI to cell service providers at all, voluntarily or otherwise, the court rejected the third-party doctrine as inapplicable to CSLI.[183] The court framed the relevant CSLI inquiry not as whether an individual has a reasonable expectation of privacy in a third party's records, but rather as whether an expectation of privacy in an individual's locations and movements over time is reasonable.[184] Because the specificity with which CSLI identifies cell sites allows users' locations to be tracked raises privacy concerns,[185] the court found the pertinent question to be whether users are generally aware of which specific cell sites are utilized when their phones connect to the network.[186] Finding that overall, cell phone users do not know which particular cell site transmits their communications or even the general location of nearby cells sites, cell phone users do not and cannot voluntarily convey information to their service provider.[187]

The federal circuit court opinions leave several questions critical to resolving the CSLI debate unanswered. One question is whether cell phone users forfeit any legitimate expectation of privacy in their CSLI when using a cell phone because of the third-party doctrine.[188] Conversely, the *Katz* reasonable expectation of privacy test could preserve cell phone users' privacy interest in CSLI, regardless of a third party, such as a cell service provider ultimately possessing the CSLI.[189] The issues of whether advances in cellular technology have altered societal privacy expectations[190] and whether courts and legislatures ought to consider the

182. *See Graham*, 796 F.3d at 350–51.

183. *Id*. at 354. "When a cell phone receives a call or message and the user does not respond, the phone's location is identified without any affirmative act by its user at all—much less, 'voluntary conveyance.'" *Id*. at 355.

184. *Id*. at 352.

185. *Id*. at 356.

186. *Id*.

187. *Id*. at 355–56.

188. *Id*. at 355.

189. *See, e.g.*, United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015), *cert. denied*, 2015 WL 4600402 (U.S. 2015) (noting the strength of arguments for changing underlying and prevailing law, such as the third-party doctrine and the SCA, but ultimately deferring to Congress and the state legislatures on enacting those changes).

190. *See, e.g.*, In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013) (recognizing that "technological changes can alter societal expectations of privacy" and sympathizing with "cell phone users . . . reasonably want[ing] their location information to remain private .

strong likelihood of future technological advances when articulating these modern privacy expectations also remains unclear.[191] This remaining uncertainty can be attributed at least in part to the limited holdings that every circuit court has issued. As CSLI challenges surface in lower-level state courts, however, states are beginning to articulate their own CSLI standards of proof and rationales.

III. STATES ATTEMPT TO RESOLVE THE CSLI CONTROVERSY

As state courts began ruling on governmental access to CSLI, a divide similar to that of federal courts has emerged over whether privacy protections for CSLI should be afforded to individuals.[192] Some states have relied on their state constitutions, which provide greater privacy protections than the Fourth Amendment, to afford additional protections to their citizens.[193] Other states have enacted their own state versions of the ECPA, which explicitly require a warrant for CSLI, and more states are debating similar action.[194] Unfortunately, both the Louisiana judiciary and legislature have neglected to react to privacy concerns in the active manner that other states have. Instead, Louisiana has left its citizens vulnerable to privacy threats by maintaining a low standard for law enforcement to obtain CSLI.

A. CSLI Standards Applicable in Other Jurisdictions

Courts in several states have recognized a reasonable expectation of privacy in CSLI and have held that a warrant based on probable cause is the appropriate standard.[195] The highest state courts in Massachusetts and

---

. . ."); *Davis*, 785 F.3d at 512 (acknowledging that "use of cell phones is ubiquitous" today and as a result, "some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government").

191. *Compare* In re Application of the United States for Historical Cell Site Data, 724 F.3d at 615 ("Recognizing that technology is rapidly changing, we decide only the narrow issues before us."), *with Graham*, 796 F.3d at 351 ("The intense competition among cellular networks provides ample reason to anticipate increasing use of small cells and, as a result, CSLI of increasing precision. We must take such developments into account.").

192. *See generally* State v. Earls, 70 A.3d 630 (N.J. 2013); Commonwealth v. Wyatt, No. 11-00693, 2012 WL 4815307 (Mass. Aug. 7, 2012); Tracey v. State, 152 So. 3d 504 (Fla. 2014).

193. *See generally Earls*, 70 A.3d 630; *Wyatt,* 2012 WL 4815307.

194. McKeown, *supra* note 154, at 2054–55.

195. *See generally Earls*, 70 A.3d 630; *Wyatt*, 2012 WL 4815307; *Tracey*, 152 So. 3d 504. In *Tracey v. State*, the Florida Supreme Court relied on the Fourth

New Jersey relied on their respective state constitutions to afford these greater privacy protections.[196] These courts have recognized the reasonable expectation of privacy in the increasing level of detailed information that cell phones can reveal about an individual's personal life and the indispensable nature of cell phones in modern society.[197] Consequently, both states' courts have held that the police must obtain a warrant based on probable cause before obtaining CSLI unless they have met an exception to the warrant requirement.[198] Both courts viewed the use of CSLI as a way of effectively transforming a cell phone into a GPS tracking device because the information that both convey allows an individual's daily movements to be tracked and disclosed.[199] The courts also rejected the third-party doctrine approach, noting that CSLI is not a voluntary disclosure because cell phone users do not take any affirmative or overt action to convey their CSLI to cell service providers.[200] Users can avoid conveying location information only at the price of not using a cell phone, which has become a personal and professional necessity for the majority of the population.[201] In both cases, however, the courts were careful to restrict their holdings squarely within the confines of their state constitutions and declined to extend their holdings to the Fourth Amendment.[202]

Some state legislatures have passed legislation governing CSLI disclosure procedures to actively protect CLSI private interest. In 2013, Montana became the first state to enact legislation that requires law enforcement to obtain a warrant to access CSLI.[203] The law is comprehensive

---

Amendment in recognizing a reasonable expectation of privacy in CSLI. 152 So. 3d at 510–11.

196. *Earls*, 70 A.3d at 644; *Wyatt,* 2012 WL 4815307 at *2.

197. *Id*.

198. *Earls*, 70 A.3d at 644; *Wyatt*, 2012 WL 4815307 at *7.

199. *Earls*, 70 A.3d at 642; *Wyatt*, 2012 WL 4815307 at *2.

200. *Earls*, 70 A.3d at 643; *Wyatt,* 2012 WL 4815307 at *6.

201. *Earls*, 70 A.3d at 643; *Wyatt*, 2012 WL 4815307 at *6.

202. *Earls*, 70 A.3d at 644; *Wyatt.* 2012 WL 4815307 at *2. Article I, Paragraph 7 of the New Jersey Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue except upon probable cause." N.J. CONST. art. I, § 7. Article XIV of the Massachusetts Declaration of Rights provides: "Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation." MASS. CONST. art. XIV.

203. Wackman, *supra* note 11, at 316.

for several reasons. One is that it establishes a clear burden of proof.[204] Another is that the law enumerates various circumstances in which the government's failure to obtain a search warrant will be justified, such as when a cell phone is reported stolen by the owner, when the government responds to a cell phone user's call for emergency services, and when a life-threating situation exists.[205] The law establishes bright-line rules for situations in which law enforcement obtains CSLI without a warrant and no warrant exceptions apply. In these scenarios, the law prohibits CSLI from being "used in an affidavit of probable cause in an effort to obtain a search warrant," and it will not be admissible "in a criminal, civil, or administrative proceeding."[206] The violator is also assessed a civil fine.[207] Several other states have followed Montana's example by passing similar legislation.[208] Over a dozen other state legislatures, including Louisiana's neighbor, Texas, have taken strides toward updating their laws to require warrants for CSLI.[209] The recent legislative movement among state legislatures further supports the notion that societal privacy expectations are evolving to include interests in keeping CSLI confidential.[210]

B. The Lack of a Clear Standard in Louisiana

Although many other states have reevaluated privacy interests in light of technological advancements, Louisiana has not. Louisiana law enforcement practices pose an even greater threat to privacy interests than the procedures that the SCA outlines because law enforcement routinely

204. 2013 Mont. Laws Ch. 394 (H.B. 603) (codified at MONT. CODE ANN. 46-5-110 (West 2016)).

205. *Id.*

206. *Id*.

207. *Id*.

208. Hanni Fakhoury, *A National Consensus: Cell Phone Location Records Are Private*, ELECTRONIC FRONTIER FOUND. (July 29, 2014), https://www.eff.org/deeplinks/2014/07/constitutionally-important-consensus-location-privacy [https://perma.cc/D5R4-GLHM]. Colorado, Maine, and Minnesota have passed statutes governing historical CSLI. *Id.* Indiana, Virginia, and Wisconsin enacted statutes governing real-time CSLI. *Id.*

209. Somini Sengupta, *With Montana's Lead, States May Demand Warrants for Cellphone Data*, N.Y. TIMES (July 2, 2013, 5:24 PM), http://bits.blogs.nytimes.com/2013/07/02/with-montanas-lead-states-may-demand-warrants-for-cellphone-data/?_r=0 [https://perma.cc/H6HF-5U6Q].

210. *See* Fakhoury, *supra* note 208.

accesses CSLI with ordinary subpoenas.[211] To obtain CSLI under the subpoena standard, Louisiana law enforcement need show only that the information it seeks is relevant or necessary to the case.[212] Prosecutors frequently use subpoenaed CSLI as evidence to convict defendants.[213]

Louisiana courts consistently allow CSLI to be admitted into evidence, but rarely give consideration about whether such a low standard of proof is an unlawful violation of Louisiana citizens' privacy rights and interests.[214] In *State v. Marinello*,[215] the defendant objected to the introduction of his cell phone records into evidence because the state should have been required to obtain a warrant for the records, rather than use a subpoena.[216] The court quickly dismissed this argument, however, and held that the subpoena was sufficient.[217] Because the records were kept in the cell service provider's ordinary course of business for billing and troubleshooting purposes, and because the data was limited to historical CSLI, the records implicated neither Fourth Amendment privacy protections nor Louisiana Constitution Article 1, Section 5 privacy protections.[218]

The defendant in *Marinello* also advanced a statutory law based argument, which the court rejected. Specifically, the defendant argued that the Louisiana Pen Register Statutes required the state to apply for the information.[219] Citing to Louisiana Revised Statutes Section 15:1302(15), the court ruled that the Pen Register statute specifically excludes CSLI.[220] Louisiana's Pen Register and Trap and Trace statutes provide that law enforcement may apply for a court order authorizing the use of a pen register or trap and trace device upon certification that "the information sought is relevant to an ongoing felony criminal investigation" and a recital of "facts or information constituting the reasonable suspicion upon which the application is based."[221] On its face, the Louisiana version of the Pen

---

211. *See, e.g.*, State v. Banks, No. 12-135, 2012 WL 5416967 (La. Ct. App. Nov. 7, 2012); State v. Bone, 107 So. 3d 49 (La. Ct. App. 2012); State v. Jackson, 132 So. 3d 516 (La Ct. App. 2014).

212. Bank of New Orleans and Trust Co. v. Reed Printing & Custom Graphics, 399 So. 2d 1260, 1261 (La. Ct. App. 1981).

213. *See, e.g.*, *Banks*, 2012 WL 5416967; *Bone*, 107 So. 3d 49; *Jackson,* 132 So. 3d 516.

214. *Id*.

215. 49 So. 3d 488 (La. Ct. App. 2010).

216. *Id*. at 508–09.

217. *Id*. at 509.

218. *Id*. at 510.

219. *Id*.

220. *Id*.

221. LA. REV. STAT. ANN. § 15:1314 (2016).

Register statute appears to govern real-time CSLI in the same way that the federal Pen Register statute does. The *Marinello* opinion, however, suggests that the Louisiana Pen Register statute is wholly inapplicable to CSLI because of Louisiana Revised Statute Section 15:1302(15), which defines the term "pen register" for the chapter's purposes. The revised statute excludes from the meaning of "pen register" devices that a cell service provider uses "in the ordinary course of the provider's . . . business" for purposes including "billing or recording as an incident to billing for communications services" or "other ordinary business purposes."[222] Because cell towers generate cell tower records, which a cell service provider uses in the ordinary course of its business, the *Marinello* court concluded that CSLI does not fall within the ambit of the Louisiana Pen Register statute.[223]

The ease with which law enforcement accesses and utilizes CSLI to generate detailed accounts of a person's movements over time poses a serious threat to personal privacy. Knowing a person's location over time reveals who individuals are and what they value.[224] Furthermore, this investigation occurs without alerting individuals that law enforcement is tracking them. The Louisiana courts' reluctance to fully address CSLI privacy concerns coupled with the lack of clear legislative guidelines governing compelled CSLI disclosure has resulted in an unclear area of the law that fails to adequately protect the privacy interests of Louisiana citizens.

IV. SOLVING THE LOUISIANA CSLI PROBLEM

Current Louisiana statutory law sets a low standard for law enforcement to obtain CSLI.[225] Dramatic technological advances, particularly in the context of cellular technology, have resulted in an evolution of societal privacy expectations, which include privacy interests in the locations individuals visit, those with whom individuals associate, and other personal activities, regardless of the decision to carry a smartphone.[226] Louisiana

222. LA. REV. STAT. ANN. § 15:1302(15) (2016).

223. *Marinello*, 49 So. 3d at 510.

224. *See id*.

225. *See, e.g.*, LA. REV. STAT. ANN. § 15:1315 (2016).

226. A recent Pew Research Center survey shows that 91% of adults agree or strongly agree that "consumers have lost control over how their personal information is collected and used by companies." MARY MADDEN, PEW RES. CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 3 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [https://perma.cc/3GJA-G32P]. The survey further

law should also advance to provide adequate protections for these recently emerging privacy interests, and both the Louisiana courts and the Louisiana legislature have a role to play in ensuring this change.

A. Expansive Constitutional Interpretation

Similar to the superior courts in New Jersey and Massachusetts, Louisiana courts should interpret the Louisiana Constitution to provide a greater level of CSLI privacy protections to Louisiana citizens. Article 1, Section 5 of the Louisiana Constitution offers greater privacy protections than the Fourth Amendment of the United States Constitution because it incorporates language that supplies a separate right of privacy, as well as an express protection of property, communications, houses, papers, and effects.[227] The drafters knowingly and intentionally incorporated this language in an effort to make the Louisiana Constitution more expansive than the United States Constitution's Fourth Amendment.[228] As a result of this additional language, "[t]he traditional guarantee against unreasonable searches and seizures is cemented and expanded."[229] Thus, based on the additional language in Article 1, Section 5, constitutional interpretations providing for greater privacy protections are not only plausible, but also were intended by the drafters.

One interpretation of the Louisiana Constitution that Louisiana courts should adopt to provide privacy protections for CSLI focuses on the language in Article 1, Section 5 that grants an affirmative right to privacy. Professor Lee Hargrave, principal architect of the Louisiana Constitution and author of *The Louisiana Constitution: A Reference Guide*,[230] explained that the "key element" of this right to privacy is that "the invasions of privacy must be unreasonable to merit constitutional protection."[231] In evaluating the reasonableness of a particular privacy invasion, courts are given "flexibility to determine which invasions of privacy are supported

---

revealed that 82% of adults feel that the details of their physical location that cell phone GPS tracking reveals is at least "somewhat sensitive," and half of adults consider this information "very sensitive." *Id*. at 34.

227. "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy." LA. CONST. art. I, § 5.

228. *See* Lee Hargrave, *The Declaration of Rights of the Louisiana Constitution of 1974*, 35 LA. L. REV. 1, 20 (1974).

229. *Id*.

230. *W. Lee Hargrave*, LSU PRESS, http://lsupress.org/authors/detail/w-lee-hargrave/ (last visited Oct. 25, 2015).

231. Hargrave, *supra* note 228, at 21.

by sufficient societal interests to be considered reasonable."[232] "[T]he purpose of the convention in expanding the individual's protections in this area beyond the existing law" guides this inquiry.[233] The congressional debates surrounding Article 1, Section 5 at its enactment further support "a desire to go far beyond federal standards and to prevent the use of evidence obtained by private persons in violation of the guarantees of the section."[234] The purposeful enlargement of the exclusionary rule further supports the idea that the framers of Article 1, Section 5 intended to provide expansive privacy protections.[235]

Individuals do not buy cell phones to use as tracking devices, nor do they reasonably expect that the government will use their cell phones in such a manner.[236] Rather, cell phone users expect the freedom to move about in relative anonymity without the government keeping an individualized turn-by-turn itinerary of their whereabouts.[237] To safeguard privacy interests in the sum of an individual's movements, Louisiana courts should adopt an expansive interpretation of Article 1, Section 5 of the Louisiana Constitution.

B. A Legislative Response

The Louisiana legislature should be proactive in creating laws that protect Louisiana citizens' privacy interests in CSLI. As Justice Alito suggests in his concurrence in *Jones*, the best solution to privacy concerns involving dramatic technological change is legislative.[238] A legislative body is "well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and safety in a comprehensive way."[239] The Louisiana legislature is well suited to take action because the legislature is the governmental body most connected to Louisiana citizens. The Louisiana legislature can communicate directly with its constituents, seek input regarding public opinion of CSLI tracking, and then incorporate these views into its actions. If public opinion changes or CSLI technology advances further, the Louisiana legislature can respond quickly by conducting hearings and investigations and drafting new legislation.[240]

232. *Id*.
233. *Id*.
234. *Id*. at 22.
235. Hargrave, *supra* note 228, at 23–24.
236. State v. Earls, 70 A.3d 630, 632 (N.J. 2013).
237. United States v. Graham, 796 F.3d 332, 348 (4th Cir. 2015).
238. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).
239. *Id*.
240. Wackman, *supra* note 11, at 317.

Louisiana needs a comprehensive statutory scheme to carve out specific exceptions to the warrant requirement and establish a clear suppression remedy. The lack of an adequate suppression remedy under Louisiana law or the SCA is problematic. Currently, if law enforcement collects CSLI under a flawed, conclusory, or false court order, no mechanism is in place to prevent this evidence from being used to prosecute a defendant.[241] A specific, clear suppression remedy, similar to that set forth in Montana's law, would discourage the prosecutor's use of tainted CSLI evidence.

A clear, straightforward statute with easily administrable standards and clear guidelines also benefits law enforcement because in the midst of high-stakes investigations, an easily understandable statute is likely to deter mistakes or abuse by law enforcement.[242] The benefit of placing the decisional authority in a neutral, detached magistrate would also alleviate concerns about police abuse of CSLI practices. A detached magistrate's scrutiny is a more reliable safeguard than the hurried judgment of a law enforcement officer "engaged in the often competitive enterprise of fettering out crime."[243] Moreover, such legislation would be consistent with the expansive constitutional interpretation of Article 1, Section 5. Law enforcement, as well as society in general, has a strong interest in the prompt apprehension of suspects,[244] especially in a way that responsibly allocates scarce investigative resources.[245] Citizens have a competing interest, however, in being free from intrusive CSLI investigative techniques that can reveal their private information when law enforcement's suspicion of their involvement in criminal activity fails to meet probable cause.[246] Cell phone users are common today, but individuals generally do not purchase cell phones believing that doing so automatically provides law enforcement with ample opportunity to compile a comprehensive record of their personal habits.[247] Conditioning the use of a cell phone, which has become a necessity to many Americans, on individuals' willingness to permit the government to track their movements without probable cause is also unreasonable.[248]

Absent an exception to the warrant requirement, requiring law enforcement to obtain a warrant based on probable cause before obtaining CSLI would likely burden law enforcement to a minimal degree. The benefits of adopting this practice, however, such as an increase of public trust, would

241. *Id*. at 314–15.
242. *Id*. at 312.
243. *Id*. at 317–18.
244. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).
245. *Id*.
246. Freiwald, *supra* note 65, at 698.
247. Wackman, *supra* note 11, at 311–12.
248. *See* Curtis, *supra* note 12, at 89.

outweigh the slight inconvenience the warrant requirement may impose on law enforcement.[249] Therefore, a comprehensive statutory scheme requiring a warrant based on a showing of probable cause and other attributes would effectively balance Louisiana citizens' privacy rights, public safety, and security.[250]

CONCLUSION

Cellular technology has advanced to a level that allows for CSLI tracking with nearly the precision of a GPS. As cell service providers continue competing to provide the most reliable and capable cellular networks for their subscribers, CSLI will continue to advance. CSLI will become more precise and thus more valuable to prosecutors and, more importantly, more convincing for juries. The prosecutorial value of CSLI underscores the importance of implementing warrant requirements, which will insulate CSLI evidence from police abuse. High-stakes criminal investigations in which investigators and prosecutors who use CSLI are under significant pressure to close cases are precisely the circumstances in which judicial oversight and legislative clarity are most needed.[251] Current federal and Louisiana law governing CSLI are inadequate to confront this reality.

In today's world, the wish to keep their movements private leaves Louisiana citizens who desire and need to stay connected and informed with no option other than to forego cellular technology altogether.[252] Louisiana courts' expansive interpretation of the constitution to provide for additional CSLI privacy protections is imperative. Equally important is the Louisiana legislature's creation of a comprehensive statutory scheme governing the specifics of CSLI, from the burden of proof required to the consequences resulting from failure to comply with that burden. This constitutional and statutory probable cause solution will protect the privacy rights of Louisiana citizens and provide clear guidelines to law enforcement without hindering its ability to investigate and prosecute violations of the law effectively.

Shannon Jaeckel[*]

---

249. Wackman, *supra* note 11, at 318.

250. *See Reforming the ECPA*, *supra* note 37, at 1.

251. *See* discussion *supra* Part I.B.

252. *See* Corbett, *supra* note 13, at 227.

* J.D./D.C.L., 2017, Paul M. Hebert Law Center, Louisiana State University, This Comment is dedicated to my family for always supporting and encouraging me. Special thanks to Professor P. Raymond Lamonica for his guidance throughout the writing process and to everyone on the *Louisiana Law Review* for their thoughtful edits.