Barry Law Review

Volume 22
Issue 1 *Fall 2016*

Article 4

4-20-2017

Find My Criminals: Fourth Amendment Implications of the Universal Cell Phone "App" that Every Cell Phone User Has but No Criminal Wants

Christopher Joseph

FIND MY CRIMINALS: FOURTH AMENDMENT IMPLICATIONS OF THE UNIVERSAL CELL PHONE "APP" THAT EVERY CELL PHONE USER HAS BUT NO CRIMINAL WANTS

Christopher Joseph[*]

INTRODUCTION

Two men were out one Friday evening, perhaps beginning a weekend of fun, and drove to meet Kendrick Herring.[1] Once all the men were together, Herring began talking with the two men; shortly thereafter, the evening took a deadly turn when Herring produced a .45 caliber handgun and began shooting at the two men, hitting them both.[2] The frightened and wounded victims fled the area and managed to make it to one of their homes; one man eventually died from his gunshot wounds, but the other survived, having been struck in one of his arms.[3] The police began investigating as soon as they were notified, and they managed to obtain Herring's cell phone information from the surviving victim.[4] Using this information and operating under exigent circumstances, the police were able to obtain Herring's real-time cell phone location data, which allowed them to quickly locate Herring and secure key evidence to support his conviction—namely, the handgun used in the murder and the cell phone Herring used to communicate with the two men prior to their meeting.[5]

Despite the heinous nature of Herring's crime, the highlighted issue in that case was not whether Herring murdered one man and attempted to murder another; instead, the focus was centered on whether the police were allowed to obtain the location of Herring's cell phone without a warrant following these events.[6] Given that approximately ninety-two percent of American adults own a mobile phone of

* J.D. Candidate, 2017, Barry University School of Law; M.S. Criminal Justice, University of Central Florida, 2008; B.S. Computer Engineering, University of Central Florida, 2005. Sergeant, Orange County Sheriff's Office, Orange County, Florida. Certified Forensic Computer Examiner, International Association of Computer Investigative Specialists. Thanks to my faculty advisor Eang Ngov, and to my legal research and writing professor Helia Hull, who provided encouragement and assistance throughout my law school career. Also, I extend my gratitude to my brothers and sisters in law enforcement, who strive to fight a never-ending battle on an ever-changing battlefield.

1. Herring v. State, 168 So. 3d 240, 242 (Fla. Dist. Ct. App.), *reh'g denied* (Fla. Dist. Ct. App.), *review dismissed*, 173 So. 3d 966 (Fla. 2015).
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.* Ultimately, the court held that although the government claimed it was operating under exigent circumstances, it had failed to sufficiently demonstrate such an exigency. *Id.* at 244.
6. *See Herring*, 168 So. 3d at 243 (reviewing whether police were allowed to obtain the location of Herring's cell phone without a warrant).

some kind (up from sixty-five percent just over a decade ago),[7] concerns about the government conducting warrantless tracking of a cell phone are certainly justified.[8] This is especially true because using a cell phone's location for electronic tracking has become a routine tool in law enforcement, exceeding the use of both wiretaps and global positioning satellite (GPS) tracking.[9] However, using this valuable tool allows police to track and apprehend dangerous criminals like Herring within the span of hours,[10] instead of allowing them to remain at large, potentially committing other crimes.

As is commonly the case with competing interests, the struggle to balance concerns about individual privacy against the need for public safety and effective law enforcement has led to varying decisions in different jurisdictions—especially because the Supreme Court of the United States left this precise issue open.[11] For example, some courts have concluded that the government is required to obtain a search warrant based on probable cause before obtaining the real-time location of a cell phone[12]—the Florida Supreme Court being among them.[13] However, other courts have held that a search warrant is not required in order to obtain or use such information, in many cases because the information obtained was limited to the defendant's travels on public roadways,[14] or because the cell phone's location information is voluntarily disclosed to a third party.[15] Adding to the confusion, whether a warrant is required for real-time location information could depend on whether the information obtained will be used in a state or federal court; in Florida, while state courts have held that a warrant is required,[16] federal courts faced with the

7. Monica Anderson, PEW RESEARCH CTR., TECHNOLOGY DEVICE OWNERSHIP: 2015 5 (2015), http://www.pewinternet.org/files/2015/10/PI_2015-10-29_device-ownership_FINAL.pdf.

8. *See* Adam Serwer, *The US Government Can Track Your Location at Any Time Without a Warrant*, MOTHER JONES (August 16, 2012), http://www.motherjones.com/mojo/2012/08/court-warrant-cellphone-gps-data (discussing concerns about the government tracking cell phones without a warrant, including invasions of reasonable expectations of privacy).

9. Julia Angwin & Scott Thurm, *Judges Weigh Phone Tracking*, WALL ST. J. (Nov. 9, 2011), http://www.wsj.com/articles/SB10001424052970203733504577024092345458210.

10. *Herring*, 168 So. 3d at 242. The police began tracking Herring's cell phone at 2:50 a.m., and he was apprehended at 4:00 a.m. the same day. *Id.*

11. United States v. Jones (*Jones II*), 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (pointing out that physical intrusion upon a vehicle decided the case, but expressing concerns over forms of surveillance which do not require a physical trespass); Serwer, *supra* note 8 (noting that *Jones II* "avoided concluding whether or not a GPS in a phone would similarly require a warrant" as did placing a GPS device on a vehicle).

12. *See, e.g.*, State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (imposing a warrant requirement in order to obtain the real-time location of a cell phone); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 583 (D. Md. 2011) (same); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (same).

13. Tracey v. State, 152 So. 3d 504, 511 (Fla. 2014) ("[T]he use of real time cell site location information to track Tracey violated the Fourth Amendment because probable cause was required, but not provided.").

14. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 777–78 (6th Cir. 2012) (holding that defendant had no expectation of privacy in the location of his cell phone because the police could have obtained the same information by following his vehicle); United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), *cert. granted and judgment vacated on other grounds sub nom.*, Garner v. United States, 543 U.S. 1100 (2005) (same).

15. *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y 2013) (pointing out that cell phone users "cannot possibly labor under the belief that their location is somehow kept secret" after being disclosed to service providers and thus users cannot maintain a reasonable expectation of privacy as to their location).

16. *See, e.g.*, *Tracey*, 152 So. 3d at 511.

same issue have held that a search warrant is not required.[17] Finally, whether probable cause is required in order to obtain historical location information is also not clearly established among courts in different jurisdictions. Some courts require a warrant when the requested records cover "a sufficiently long—albeit undefined—period of time" but do not require one when the request is shorter than this undefined time frame.[18] However, a majority of courts have concluded that historical location information can be obtained without a warrant regardless of the time period covered in the request for information.[19] Given the lack of direction on how to obtain and use cell phone location information in compliance with the Fourth Amendment, and the increasing prevalence of its use in law enforcement investigations, a definitive answer from the Supreme Court may be necessary in order to provide appropriate direction to law enforcement officials.

This note explores the Fourth Amendment implications behind law enforcement obtaining and using cell site location information (CSLI) to conduct criminal investigations, and suggests legal arguments for law enforcement to obtain and use CSLI without obtaining a warrant. First, in Part I, this note provides background information regarding CSLI. The discussion explains how CSLI is generated and briefly explores the history of the acquisition and use of historical and real-time CSLI in the courts. Next, Part II of this note argues that under existing precedent, a search warrant is not required in order to obtain and use CSLI when the government is conducting criminal investigations. The foundation for this argument rests primarily on Supreme Court jurisprudence, with added insight provided from state courts and other federal courts.

Finally, Part III of the note argues that even if a search warrant is thought to be required in order for law enforcement to obtain CSLI, several exceptions to the warrant requirement should apply in the context of CSLI search warrants. Specifically, the note discusses the applicability of three exceptions: exigent circumstances in hot pursuit of a criminal suspect, exigent circumstances involving public safety, and what is termed as the "arrest warrant exception" recognized in *Payton v. New York*,[20] which (as originally established) allows the police to conduct a warrantless entry of defendant's residence if the police have an arrest warrant for a defendant and have a reason to believe that the defendant is within the home.[21]

This note does not discuss the use of GPS in order to locate a phone, except to the extent that previous court decisions bear on the analysis of using CSLI. Notably, because GPS and CSLI are both capable of persistent and fairly precise tracking of

17. *See, e.g.*, United States v. Sereme, No. 2:11-CR-97-FTM-29SPC, 2012 WL 1757702, at *10 (M.D. Fla. Mar. 27, 2012) *report and recommendation adopted*, No. 2:11-CR-97-FTM-29SPC, 2012 WL 1757271 (M.D. Fla. May 16, 2012) *aff'd sub nom.* United States v. Hyppolite, 609 F. App'x 597 (11th Cir. 2015).

18. United States v. Graham, 846 F. Supp. 2d 384, 388–89 (D. Md. 2012), *aff'd but criticized*, 796 F.3d 332 (4th Cir. 2015) *reh'g en banc granted,* No. 12-4659 L, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

19. *Id.* at 389.

20. Payton v. New York, 445 U.S. 574 (1980).

21. *Id.* at 603. The definition of the "arrest warrant exception" as outlined here is something of a misnomer in that it is not a true exception to the warrant requirement; a warrant is still required in order to make use of this "exception." However, it is unique in that *Payton* allows an arrest warrant to be used as a search warrant in limited circumstances.

a phone,[22] any ruling on the issue of tracking a phone using CSLI would likely be applicable to tracking a phone using GPS, and vice versa.[23] Further, this note also does not discuss the applicability of state or federal statutes to obtaining and using CSLI; ultimately, while a violation of an applicable statute may subject a law enforcement agency to civil and criminal liability, many of these statutes explicitly rule out application of the exclusionary rule as a remedy.[24]

I. BACKGROUND OF CELL SITE LOCATION INFORMATION

A. How Cell Site Location Information Works

To understand the controversy surrounding the use of CSLI, it is important to understand exactly how CSLI is generated—in other words, how it works. Cell phones use radio waves to communicate between the phone itself and the cellular network.[25] Service providers maintain radio base stations, called cell sites, spread throughout their coverage area.[26] When a cell phone is turned on, it connects to a local cell site, and then periodically checks the signal strength of the nearest site.[27] When a phone moves away from this first site and is closer to one with a stronger signal, the phone is "handed off" to the new cell site.[28] Because of this, the service provider generally knows which cell site any given phone is associated with at any given time.[29] The size of the area served by a cell site determines the accuracy of CSLI when attempting to determine the location of a connected phone.[30] Thus, in rural areas, CSLI may not be as useful when attempting to locate someone, since there are fewer cell sites that serve larger coverage areas.[31] However, in an urban area with many cell sites, a phone could potentially be located within a few hundred feet due to a smaller coverage area;[32] in fact, where microcells[33] are present, a phone

22. Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 495 (2012).

23. In fact, at least one court noted that cell site location information allows for location precision approaching that of GPS. *In re* Application of the U.S. for Historical Cell Site Data (*Historical Cell Site Data I*), 747 F. Supp. 2d 827, 837 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013). Further, in that case, the court used decisions analyzing the use of GPS in order to reach its conclusion about how CSLI can be used, given the similarities in what both sources reveal. *Id.* at 845–46.

24. *See, e.g.*, Tracey v. State, 152 So. 3d 504, 510 (Fla. 2014) (noting that despite a violation of the Florida statute governing the acquisition and use of CSLI, the exclusionary rule does not apply; this was the same for violations of the federal Stored Communications Act).

25. *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. 20 (2010) [hereinafter *Hearing*] (statement of Matt Blaze, Associate Professor, University of Pennsylvania).

26. *Id.*

27. Angwin & Thurm, *supra* note 9, at illus. "Cell-Tower Surveillance."

28. *Hearing*, *supra* note 25, at 20.

29. Angwin & Thurm, *supra* note 9, at illus. "Cell-Tower Surveillance."

30. CTR. FOR DEMOCRACY & TECH., *Cell Phone Tracking: Trends in Cell Site Precision* 1 (2013) [hereinafter CDT], https://www.cdt.org/files/file/cell-location-precision.pdf.

31. Angwin & Thurm, *supra* note 9, at illus. "Cell-Tower Surveillance."

32. *Id.*

33. Microcells, picocells, and femtocells are all low-power small cell sites that allow service providers to increase their network coverage; they provide service to areas as large as 2000 meters to as small as 10 meters. CDT, *supra* note 30, at 2.

could be located as accurately as identifying the individual floor or room within a building.[34] Thus, especially in urban areas, the accuracy of CSLI can approach GPS-level precision.[35]

Besides providing the general location of a phone as somewhere within the coverage area of a cell site, new technology enables service providers to potentially locate a phone's position within the coverage area.[36] Using the time the phone arrives within the coverage area, as well as the angle at which the signal arrives, can allow a phone's latitude and longitude to be located with a level of accuracy that also approaches the accuracy of GPS.[37] This calculation can be made even when the phone is not actively making a phone call or otherwise communicating with the network, so long as it is turned on; however, whether service providers routinely track and record this information varies among service providers.[38] Unlike GPS, CSLI does not depend on any special hardware or programs within the user's phone; rather, it is calculated based on data collected and analyzed at the cell sites themselves.[39] Thus, the position of every cell phone active in a network could be calculated without the knowledge or cooperation of the phone's owner.[40]

Given that the majority of the adult American population owns a cell phone,[41] the ability to determine the location of one of these adults, even without GPS-level precision, is a valuable tool for law enforcement. Over time, law enforcement has

34. Angwin & Thurm, *supra* note 9, at illus. "Cell-Tower Surveillance."

35. CDT, *supra* note 30, at 4. However, it is important to note that there is a difference between the possibility of obtaining data that near-GPS precision location information and actually obtaining that information. The author has over ten years of law enforcement experience, and in executing several search warrants to obtain CSLI, he noted that historical and real-time CSLI obtained in practice could not be fairly described as containing near-GPS precision information. Historical CSLI always includes only the location and sector of the cell tower servicing the phone. Even while "pinging" a phone and obtaining real-time CSLI, the author has noted that the locations obtained cover several residential units, especially in urban areas.

36. *Hearing*, *supra* note 25, at 26.

37. *Id.*

38. *Id.* Many service providers do keep track of CSLI in general because it provides a significant benefit to them—namely, it allows them to "identify where new infrastructure is required, where old infrastructure is redundant, and how and where their customers use different wireless services." *Id.* at 27. Keeping track of this information not only "makes good engineering sense," but also, this information is "extraordinarily valuable for network management, marketing, and developing new services." *Id.* at 27–28. However, many service providers only keep this information, known as "registration data," for about ten minutes. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 534 (D. Md. 2011).

39. *Hearing*, *supra* note 25, at 22.

40. *Id.* This is somewhat misleading, because although the actual calculation of the user's location may be done without the user's express knowledge or cooperation, the knowledge of how to avoid transmitting one's location via cell phone is "widely known and readily accessible"; the user simply has to turn off his phone. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 139 (E.D.N.Y. 2013). Further, the user knows that when the phone is turned on, cell phone providers are calculating and collecting his location information. *Id.* at 141–42. It would appear then that a user not knowing the exact moment that his location is calculated is of little consequence, as he is knowingly allowing this information to be transmitted and collected by allowing the phone to remain on.

41. "Roughly nine-in-ten American adults (92%) own a mobile device of some kind." ANDERSON, *supra* note 7, at 5. In 2015, there were approximately 321 million adults in the United States. *See QuickFacts*, U.S. CENSUS BUREAU, http://www.census.gov/quickfacts/table/PST045215/00 (last visited Oct. 10, 2016). This means that there are approximately 295 million adult cell phone owners in the United States.

made frequent use of this tool;[42] the types of requests made and a brief history of CSLI's use in criminal investigations completes the picture of the controversy surrounding the use of this technological advancement.

B. The History of Cell Site Location Information in the Courts

Although cell service providers generate CSLI in the aforementioned manner, the information is not simply available to the government for the taking.[43] Instead, law enforcement can make two different types of CSLI requests through the courts: one for historical CSLI and one for real-time (or prospective) CSLI.[44] Historical CSLI is information that cell phone providers have already collected and logged over a specified period of time, at least at the time the request for the information is made.[45] Real-time CSLI is information that is obtained going forward from the date of a court's order.[46] Regardless of whether law enforcement requests real-time or historical CSLI, the information obtained is identical in both cases.[47] This information includes the date and time of communications made and received using the phone, the telephone numbers involved in these communications, the cell tower to which the phone was connected, and the duration of the call, among other information.[48] Although the application of information that law enforcement could obtain from CSLI is clear, what has historically been unclear is the appropriate standard that law enforcement must satisfy in order to obtain it.

Perhaps the first published decision regarding the government's use of CSLI was the Sixth Circuit's decision in *United States v. Forest*.[49] In this case, the police (after obtaining a court order) used real-time CSLI to track the defendant's movements over the roadways while they also attempted to maintain traditional, visual surveillance over the defendant's vehicle.[50] Relying primarily on the fact that the defendant's location was tracked only while he was in public, the court concluded that there was no Fourth Amendment violation because the CSLI was merely a proxy for the defendant's visually observable location.[51]

Thereafter, decisions discussing the government's use of real-time CSLI began appearing more frequently in 2005, increasing in frequency through 2010; like

42. One magistrate estimated that "federal courts alone issue 20,000 to 30,000 cellphone tracking orders annually." Angwin & Thurm, *supra* note 9.

43. In order to obtain CSLI information, the government must at least obtain a court order from a judge. 18 U.S.C. § 2703(c) (2012). In seeking such an order, the government need not demonstrate probable cause, but instead must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

44. United States v. Jones (*Jones I*), 908 F. Supp. 2d 203, 207 (D.C. Cir. 2012).

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

50. *Id.* at 947–48.

51. *Id.* at 951.

Forest, these cases concerned the use of real-time CSLI.[52] Although many of these cases were decided on statutory grounds,[53] some of the cases considered and decided whether it was appropriate for the government to obtain or use real-time CSLI after considering Fourth Amendment implications.[54] For those courts, the rationale justifying the decisions on both sides of the issues varied widely. Courts denying applications for real-time CSLI have done so generally because of the possibility that tracking the location of the cell phone would invade the target's Fourth Amendment rights by tracking the target into a constitutionally protected space.[55] Other courts reaching the same conclusion did so not necessarily because tracking the phone would reveal details about any constitutionally protected space, but instead because of an expectation of privacy a target has in the location of his cell phone.[56] Courts that have approved the use of CSLI without a warrant have done so for several reasons; these include the conclusions that a cell phone user does not have any reasonable expectation of privacy in the location data given off by the phone voluntarily,[57] and CSLI is merely a proxy for a target's visually observable location.[58]

Besides acquiring real-time CSLI to locate criminal defendants, the government also routinely sought historical CSLI as evidence—commonly to place defendants at the scene of a crime.[59] Although there were some decisions related to the acquisition and use of historical CSLI prior to 2010, the majority of the cases on this topic were decided in and after 2010.[60] Like their real-time counterparts, decisions regarding historical CSLI have articulated varying justifications. Beyond the issues involving statutory interpretation and legislative intent, a few courts have held that obtaining historical CSLI always requires a warrant because cell phone users have a

52. *See, e.g.*, *In re* Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (requesting real-time CSLI); *In re* Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & Caller Identification Sys. on Tel. Nos. (Sealed), 402 F. Supp. 2d 597 (D. Md. 2005) (same); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth. (*Pen Register & Trap/Trace Device*), 396 F. Supp. 2d 747 (S.D. Tex. 2005) (same).

53. *See, e.g.*, *In re* Applications of U.S. for an Order Authorizing Continued Use of a Pen Register & Trap & Trace with Caller Identification Device, 530 F. Supp. 2d 367, 368 (D. Mass. 2007); *Authorizing the Use of a Pen Register*, 384 F. Supp. 2d at 566; *In re* U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 140 (D.D.C. 2006).

54. *See, e.g.*, *In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

55. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011); *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & Trap & Trace Device, 396 F. Supp. 2d 294, 323 (E.D.N.Y. 2005) (quoting *Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 757).

56. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014).

57. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

58. *Id.* at 779 (quoting United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004)).

59. *See, e.g.*, United States v. Davis, 785 F.3d 498, 501 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015). The same court noted that CSLI could tell law enforcement whether the suspect was in the general vicinity of a crime. *Id.* at 518.

60. *See generally* Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015) (compiling cases that discussed obtaining or using historical CSLI, the vast majority of which were decided after 2010).

reasonable expectation of privacy in their location.[61] Interestingly, a number of courts have determined whether a Fourth Amendment violation has occurred based on the length of time covered by the records sought by the government. If the span of the time is relatively short, these courts tend to allow the government to obtain historical CSLI.[62] In contrast, if the span of time covered is relatively long, then courts holding the length of time to be important decline applications for historical CSLI.[63] However, "[a] majority of courts . . . have concluded that the acquisition of historical cell site location data . . . does not implicate the Fourth Amendment, regardless of the time period involved."[64] These courts reached this conclusion because, like the similar conclusion for real-time CSLI, "people voluntarily convey their cell site location data to their cellular providers" and thus have no expectation of privacy in that information.[65] With the case law on CSLI being in substantial disarray, it is difficult to say which rationale will ultimately prevail if and when the issue reaches the Supreme Court. However, the Court's current precedent should lead the lower courts to decide that a search warrant is not required in order to obtain any form of CSLI, be it historical or real-time.

II. A SEARCH WARRANT IS NOT REQUIRED TO OBTAIN CELL SITE LOCATION INFORMATION

The rationale for not requiring a search warrant to obtain CSLI is that, simply put, when members of law enforcement do obtain CSLI, they are not conducting a search within the meaning of the Fourth Amendment. To start, the Fourth Amendment provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and generally requires a warrant based upon probable cause to be issued in order for the government to conduct a search.[66] Early on, in order for government conduct to be deemed a search, there must have "been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[67] In *Katz v. United States* however, the Supreme Court rejected the property-based test for

61. *See, e.g.*, Commonwealth v. Pitt, No. 2010-0061, 2012 WL 927095, at *10 (Mass. Supp. Feb. 23, 2012).

62. *See, e.g.*, Commonwealth v. Estabrook, 38 N.E.3d 231, 237 (Mass. 2015) (holding that obtaining six hours of historical CSLI without a warrant does not violate the Fourth Amendment).

63. *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011) (holding that obtaining 113 days of historical CSLI without a warrant violates the Fourth Amendment); *Estabrook*, 38 N.E.3d at 238 (holding the same regarding two weeks of historical CSLI data).

64. United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012). In this case, the court considered whether the acquisition of two different periods of historical CSLI violated the Fourth Amendment, one period being 221 days. *Id.* at 387. Further, the view that the time period covered by the records sought is irrelevant to the Fourth Amendment analysis finds support in *Jones II*; there, the Court rejected the idea that the duration of government monitoring, in addition to the nature of the crime being investigated, was relevant to the analysis of whether a Fourth Amendment violation occurred. *Jones II*, 132 S. Ct. 945, 954 (2012).

65. *Graham*, 846 F. Supp. 2d at 389.

66. U.S. CONST. amend. IV.

67. Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967). Although a physical trespass is no longer required in order to constitute a search, a trespass still is sufficient to establish a search under the Fourth Amendment. *See Jones II*, 132 S. Ct. at 950.

determining when a search occurred by recognizing that "the Fourth Amendment protects people, not places."[68] Instead, the Court held that the standard for determining whether a search occurred is a two-pronged test: "first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[69] If this test is not met, no search has occurred within the meaning of the Fourth Amendment.[70]

While this test provided some answers on how to deal with potential searches and seizures that did not involve a physical trespass, it also created questions—most importantly, what expectations of privacy are reasonable? Providing guidance to answer this question, the Court has explained that a search or seizure is evaluated "under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[71] Further, "there is a 'strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is "reasonable"'" with regards to searches and seizures.[72] Beyond this general guidance, the Court has provided a solid foundation for the conclusion that obtaining both historical and real-time CSLI, pursuant to a court order not based on probable cause, does not offend the Fourth Amendment.

A. Historical Cell Site Location Information

With regard to historical CSLI, one case in particular explains why an expectation of privacy in this information is not reasonable, and thus the government is not conducting a search when obtaining it. In *Smith v. Maryland*, the Court examined a case in which the police installed a pen register at the offices of a telephone company in order to obtain the phone numbers dialed from the defendant's home in connection with a criminal investigation.[73] The government then used the evidence obtained from the pen register, as well as other evidence, to convict Smith for robbery.[74] In upholding Smith's conviction, the Court said it was doubtful

> that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone

68. *Katz*, 389 U.S. at 351.
69. *Id.* at 361 (Harlan, J., concurring).
70. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 39–40 (1988) (holding that the expectation of privacy in garbage left on the side of the public street is not objectively reasonable and consequently concluding there was no search under the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding there was no reasonable expectation of privacy with regards to observations into residential backyard from 1000 feet in the air).
71. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).
72. United States v. Watson, 423 U.S. 411, 416 (1976).
73. Smith v. Maryland, 442 U.S. 735, 737 (1979).
74. *Id.* at 738.

> company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.[75]

The Court then pointed out that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[76] This is true even if the information is being voluntarily disclosed by a person to a third party on an assumption that it will only be used for a limited purpose and is being given in confidence to the third party.[77] Importantly, when *Smith* was decided, "telephone records necessarily showed exactly where the user was—his home—at the time of the call, as the user's telephone number was tied to a precise address."[78]

The same rationale that led to the conclusion in *Smith* is easily applied to CSLI. In deciding that applications for historical CSLI should have been granted, the United States Court of Appeals for the Fifth Circuit noted that

> [a] cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. Cell phone users recognize that, if their phone cannot pick up a signal (or "has no bars"), they are out of the range of their service provider's network of towers. . . . Even if this cell phone-to-tower signal transmission was not "common knowledge," [there is] evidence that cell service providers' and subscribers' contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls. In addition, these documents inform subscribers that the providers not only use the information, but collect it. Finally, they make clear that providers will turn over these records to government officials if served with a court order. Cell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed.[79]

75. *Id.* at 742.

76. *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 449 (1963)).

77. *Smith*, 442 U.S. at 744 (citing *Miller*, 425 U.S. at 443).

78. United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

79. *In re* Application of the United States for Historical Cell Site Data (*Historical Cell Site Data II*), 724 F.3d 600, 613 (5th Cir. 2013) (internal citations omitted). *See also In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y 2013) ("Cell phone customers similarly convey geolocation data to their telephone carriers, and cannot possibly labor under the belief that their location is somehow kept secret from telecommunication carriers and other third parties."). The same case also discusses the media attention, at that time, given to the fact that the location of cell phones could be tracked, fairly easily, by businesses and members of the

In addition to noting this "common knowledge" among cell phone users, the court also pointed out that the ownership and use of a cell phone is entirely voluntary, as is the choice to obtain cell phone service from a provider that chooses to keep such records.[80] Armed with these facts, the Fifth Circuit easily concluded that CSLI is a "business record[] and should be analyzed under that line of Supreme Court precedent."[81]

Proponents of a warrant requirement for historical CSLI advance one main argument: the provision of historical CSLI to members of law enforcement allows them to obtain a "detailed and intimate picture" of a target's comings and goings—which invades the individual's right to privacy.[82] However, not only does this argument attempt to sidestep the aforementioned relevant—and binding—Supreme Court precedent, it is flawed in its own right. Historical CSLI does not paint the intimate picture of a target's comings and goings as claimed.[83] The precision of historical CSLI depends largely on the equipment available in the area,[84] because while it may be possible to calculate a person's position with near-GPS precision,[85] in most cases historical CSLI only identifies the tower that was used to route a phone call.[86] Even if the location is further refined by identifying the sector from which a phone call originated, the user could still be anywhere within the covered sector.[87] Thus, historical CSLI does not allow the government to gain the "intimate portrait of person, social, religious, medical, and other activities and interactions" claimed by those who would advance this argument.[88] This is true regardless of the amount of time covered by the government's request for records.[89]

Even if obtaining historical CSLI is a search because of the expectation of privacy, a warrant is still not necessarily required; instead, a court must determine the reasonableness of the search by balancing the intrusion on individual privacy with the need to promote legitimate governmental interests.[90] With regard to individual privacy, as previously established, there is no reasonable expectation of privacy in the business records kept by a third party.[91] Further, historical CSLI does not reveal the content of any conversation being transmitted through the phone and does not pinpoint the location of the user.[92] Additionally, safeguards for personal

---

public. *Id.* at 139–41. In particular, the court discusses the "Stalker App," which aggregated geolocation data and personal information that was *already available to the public*, conveyed there by cell phone users. *Id.* at 141.

80. *Historical Cell Site Data II*, 724 F.3d at 613.

81. *Id.* at 615.

82. *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011).

83. *Davis*, 785 F.3d at 515.

84. *See supra* Part I.A for a discussion on the different levels of accuracy of CSLI in rural and urban areas.

85. *See supra* Part I.A for a discussion on new technology that can allow a phone to be located with near-GPS precision.

86. *Davis*, 785 F.3d at 515.

87. *Id.*

88. *Id.*

89. *Id.* (noting that neither one day of historical CSLI procured in compliance with the law, nor sixty-seven days, violated the Fourth Amendment).

90. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

91. United States v. Miller, 425 U.S. 435, 442–44 (1976).

92. *Davis*, 785 F.3d at 517.

privacy are already in place; in order to ensure that the records sought actually serve legitimate government interests, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the historical CSLI sought is "relevant and material to an ongoing criminal investigation," and this information must be provided to a detached and neutral magistrate prior to the issuance of a court order.[93]

Given the minimal intrusion on individual privacy, the judicial oversight available to prevent an arbitrary invasion of privacy, and the presumed reasonableness of government action that complies with federal law,[94] the only factor left to assess is whether the information sought serves a compelling governmental interest. Law enforcement agencies nationwide use historical CSLI to investigate a wide range of crimes, including kidnapping, murder, robbery, rape, and other serious offenses.[95] Certainly, society has a compelling interest in both capturing those who commit these heinous crimes as well as quickly eliminating from suspicion those who are innocent of any wrongdoing.[96] Historical CSLI allows the police to fulfill this interest because it allows investigators to determine whether an individual was at the scene of the crime.[97] After carefully weighing all of these factors, even if obtaining historical CSLI was a search as claimed, this search is reasonable under the Fourth Amendment and a warrant is not required.[98]

This result makes sense in light of other records containing personal information available to the government without probable cause. For example, historical CSLI is certainly no more revealing (or intrusive on individual privacy) than medical records, which are available pursuant to a subpoena after the government shows their relevance to a criminal investigation.[99] In addition, the police can obtain a wide variety of records that could allow them to paint an "intimate picture" of a person's life via subpoena, including credit card statements, bank statements, purchase orders, and invoices that would reveal where a person spends his money and what he spends it on.[100] The law actually provides more protection for citizens with regards to historical CSLI because, unlike an ordinary subpoena, law enforcement officials can only obtain historical CSLI after appearing before a judge.[101] In light of all this, without regard to whether obtaining historical CSLI is a search, when the government obtains this information without a warrant, it simply cannot be held to violate the Fourth Amendment.

93. 18 U.S.C. § 2703(d) (2012).
94. *See* United States v. Watson, 423 U.S. 411, 416 (1976).
95. *Davis*, 785 F.3d at 518 (listing several categories of crimes and citing case examples).
96. *Id.*
97. *Id.*
98. *Id.*
99. *See, e.g.*, Ussery v. State, 654 So. 2d 561, 561–62 (Fla. Dist. Ct. App. 1995). Notably, the § 2703(d) court order to obtain CSLI is the equivalent of a judicial subpoena. *Davis*, 785 F.3d at 517.
100. *Davis*, 785 F.3d at 506.
101. *Id.* Ordinarily, the government can compel a witness to "produce any books, papers, documents, data, or other objects the subpoena designates" by simply filling in the blanks on a subpoena issued by the clerk without any involvement from a judge. FED. R. CRIM. P. 17(a), (c)(1).

B. Real-Time Cell Site Location Information

As with historical CSLI, the third-party doctrine outlined in *United States v. Miller*[102] dictates that when the government obtains real-time CSLI from cell service providers, it is not conducting a search within the meaning of the Fourth Amendment.[103] Simply put, a cell phone user does not have a reasonable expectation of privacy in the location data given off by his phone[104] because the user understands that his location must be conveyed as part and parcel to the provision of cell phone service.[105] Accordingly, when the government obtains a court order without probable cause to acquire real-time CSLI, it is not violating the Fourth Amendment.[106]

Besides support from the third-party doctrine, some courts have concluded that obtaining real-time CSLI without a warrant supported by probable cause does not violate the Fourth Amendment when the information revealed only describes the user's public movements.[107] In making this conclusion, these courts have relied primarily on two Supreme Court cases—*United States v. Knotts*[108] and *United States v. Karo*.[109]

In *Knotts*, the police were investigating a group of men suspected of manufacturing drugs, and placed a tracking device inside of a container of chloroform that was later purchased by one of the defendants.[110] The police used visual surveillance as well as signals from the tracking device to follow the container, which was being transported in a vehicle, to a cabin occupied by one of the defendants.[111] In deciding that the use of the tracking device did not violate the Fourth Amendment, the Court pointed to the fact that, while on the public roadways, the defendants could have been observed by law enforcement officials conducting traditional surveillance and simply following their vehicle.[112] Accordingly, there was no legitimate expectation of privacy invaded by the government.[113]

Later, in *Karo*, the government placed a tracking device inside of a container that was given to a criminal defendant and then used that device while it was inside of a private residence to confirm its location there; this confirmation was used to

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

103. *See supra* Part II.A for a full discussion on the application of the third-party doctrine to historical CSLI; for the purposes of this section, only a brief overview of the justifying rationale is provided. The applicability of the third-party doctrine makes sense for real-time CSLI, in part, because the information gained from real-time CSLI is the same as information obtained from historical CSLI, and both are business records kept by cell phone providers. *Jones I*, 908 F. Supp. 2d 203, 207 (D.C. Cir. 2012).

104. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

105. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y 2013).

106. *See id.* at 147; *In re* Application of U.S. for an Order for Disclosure of Telecomms. Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 449–50 (S.D.N.Y. 2005) (reaching the same conclusion).

107. *Skinner*, 690 F.3d at 781 (holding that there was no reasonable expectation of privacy in real-time CSLI where police tracked a cell phone that was voluntarily used while traveling on public highways).

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

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

110. *Knotts*, 460 U.S. at 278.

111. *Id.*

112. *Id.* at 285.

113. *Id.*

obtain a search warrant for the residence.[114] The Court noted that the monitoring of the tracking device occurred inside of a private residence and held that even though it was "less intrusive than a full-scale search,"[115] this activity qualified as a search for which a warrant was required.[116] Combining the holdings of *Knotts* and *Karo*, the government is free to conduct electronic surveillance of a subject while he or she travels on public thoroughfares, but it cannot use this kind of electronic surveillance to monitor the inside of a private residence.[117]

Critics, however, argue that "because cell phone users tend to take their phones with them everywhere, officers could not know in advance whether the tracking would follow the suspect into clearly protected areas" like a home.[118] Rather than impose the risk of a Fourth Amendment violation on the people, these courts impose the warrant requirement on the government.[119] This argument makes sense, since the Fourth Amendment cannot afford any protection to the people if a violation cannot be prevented before it occurs.[120] This rationale also finds some support in *Karo*, where the government argued it would be forced to obtain a warrant for all electronic surveillance cases because "[it has] no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises."[121] Although the Court did not find the government's argument compelling, it did not seem to pass judgment on such a requirement.[122]

However, the same case undermines the entire line of reasoning justifying this opposition; when the monitoring of the tracking device was found to be a Fourth Amendment violation, the Court simply struck it from the warrant and then evaluated whether the remaining information justified the issuance of the warrant.[123] Further, the Court also said, "we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."[124] The monitoring of real-time CSLI definitely has the *potential* to follow a cell phone user into his home, but this potential is not enough to impose the requirements of the Fourth Amendment.[125] Admittedly, it would behoove the government to obtain a warrant if it relies on the

114. *Karo*, 468 U.S. at 708–10.
115. *Id.* at 715.
116. *Id.* at 718.
117. This is, of course, subject to the holding in *Jones II*, which prohibits the government from performing this type of surveillance if it involves a physical trespass. *Jones II*, 132 S. Ct. 945, 949 (2012).
118. Tracey v. State, 152 So. 3d 504, 518 (Fla. 2014) (citing *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011)).
119. *See, e.g.*, *Tracey*, 152 So. 3d at 524.
120. *Id.* at 519.
121. *Karo*, 468 U.S. at 718.
122. *See id.*
123. *Id.* at 719–21.
124. *Id.* at 712.
125. Despite this, it is equally important to point out that the Fourth Amendment is designed to prevent unlawful police action rather than simply redress it after the fact. Steagald v. United States, 451 U.S. 204, 215 (1981) (citing Chimel v. California, 395 U.S. 752, 766 n.12 (1969)).

reasoning of *Knotts* and *Karo* because without one, "the government acts at its peril" and risks the suppression of evidence.[126]

Another argument for a warrant requirement relating to real-time CSLI is that it converts the user's cell phone into a tracking device, which demands compliance with rules and statutes that require a warrant to be issued upon probable cause.[127] However, acquiring real-time CSLI does not turn a user's cell phone into a tracking device; in fact, "construing 'tracking device' to encompass a cell phone is simply illogical and unworkable."[128] While it is true that a federal statute defines a tracking device as "an electronic or mechanical device [that] permits the tracking of the movement of a person or object,"[129] this confuses a device installed for the primary purpose of tracking movement with something that, incidental to its primary purpose, can be tracked or traced.[130] Moreover, interpreting tracking devices to encompass items like cell phones would have absurd results. Under this broad interpretation,

> an individual travelling by bicycle, leaving tire tracks in a muddy field; an automobile taillight, which could permit officers to follow a car at night; or the transmitter of a pirate radio station, the signal from which may be located via triangulation, would each constitute an "electronic or mechanical device which permits the tracking of the movement of a person or object."[131]

Even if obtaining real-time CSLI did convert a cell phone into a "tracking device," there would still be no Fourth Amendment violation. "The Government does not require a member of the public to own or carry a phone,"[132] so any phone that a user chooses to carry is voluntarily carried, much like the container voluntarily accepted in *Knotts*. Accordingly, tracking a phone while in public would not be a Fourth Amendment violation;[133] only tracking the phone within a private area, such as a home, would require a warrant.[134]

One final argument for a warrant requirement, and perhaps the most persuasive, has found much support and is best outlined in *Tracey v. State*.[135] There, the court embraced the argument that real-time CSLI may follow the user into his or her home, but also argued against the Court's more lenient rules established in *Smith* and

126. *In re* Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and Caller Identification Sys. on Tel. Nos. (Sealed), 402 F. Supp. 2d 597, 605 (D. Md. 2005).
127. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 537 (D. Md. 2011); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005).
128. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 149 (E.D.N.Y 2013).
129. 18 U.S.C. § 3117(b).
130. *Smartphone Geolocation Data*, 977 F. Supp. 2d at 149.
131. *Id.* at 149.
132. *Historical Cell Site Data II*, 724 F.3d 600, 613 (5th Cir. 2013).
133. United States v. Knotts, 460 U.S. 276, 281 (1983).
134. United States v. Karo, 468 U.S. 705, 718 (1984).
135. Tracey v. State, 152 So. 3d 504 (Fla. 2014).

Miller.[136] Relying on the concerns expressed in Justice Sotomayor's concurrence in *United States v. Jones*, the court in *Tracey* pointed out that

> [s]imply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes. While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction.[137]

Like the argument regarding historical CSLI, the *Tracey* court was concerned that real-time CSLI would "reveal a detailed and intimate picture of the user's life."[138] This assertion overlooks two important facts. First, the extent of "information made available is not a factor in the application of the" third-party doctrine.[139] Just like credit card records, real-time CSLI may in fact provide information beyond just the contents of the records themselves.[140] But the government can obtain many records that could allow it to paint this same "intimate" picture with just a subpoena—no warrant (or judicial oversight) required.[141] In the case of CSLI, legislative bodies have "required more before the government can obtain telephone records from a third-party business" because review by a detached and neutral magistrate is required prior to the issuance of a court order.[142] Clearly then, the ability to paint an "intimate picture" is not enough to demand that the government get a warrant before obtaining real-time CSLI.

Second, and perhaps most importantly,

> [i]t may well be that the vast expansion of data provided by individuals to third parties—along with a widespread heightened concern regarding the privacy of that data—points to a need for reexamining the third-party[] doctrine. Any such reexamination, however, is properly within the province of the Supreme Court. The Supreme Court gave us the third-party[] doctrine, and if that

136. *See generally id.* at 519–20 (arguing that, in the digital age, not all information given to third parties is exempt from Fourth Amendment protection).
137. *Id.* at 522.
138. *Id.* at 523.
139. *Id.* at 528 (Canady, J., dissenting).
140. *Id.*
141. *See, e.g.*, Ussery v. State, 654 So. 2d 561, 561 (Fla. Dist. Ct. App. 1995) (allowing the government to obtain medical records pursuant to a subpoena); United States v. Davis, 785 F.3d 498, 506 & n.9 (11th Cir. 2015) (noting that "[t]he government routinely issues subpoenas to third parties to produce a wide variety of business records, such as credit card statements, bank statements, hotel bills, purchase orders, and billing invoices" that can show the location and time of purchases as well as reveal "intimate details of daily life").
142. *Davis*, 785 F.3d at 506.

> doctrine is to be judicially altered, it should only be altered by the Supreme Court.[143]

For better or for worse, because the Court has provided us with the third-party doctrine, and because the government's acquisition of both historical and real-time CSLI without a warrant is justified by this doctrine, until the Court (or a legislative body) requires a warrant for this data, obtaining it via a court order without probable cause does not offend the Fourth Amendment.

III. EXCEPTIONS TO A WARRANT REQUIREMENT FOR CELL SITE LOCATION INFORMATION

Even though there should not be a warrant requirement for the government to obtain CSLI, what is clear currently is that the courts have differing opinions on the matter;[144] given this, the government may lose critical evidence if it obtains CSLI without first getting a search warrant based on probable cause.[145] Further, even if the lower courts were to agree that probable cause is not required for this information, the Supreme Court has yet to rule precisely on the issue, and may in fact modify the third-party doctrine outlined in *Miller* and *Smith*, as suggested by Justice Sotomayor,[146] or may make a rule specifically related to obtaining CSLI all together, separate from this doctrine.[147]

Despite any future ruling that may dub the acquisition of CSLI a search, these searches could still be reasonable in the absence of a warrant if they fall within one of the carefully delineated exceptions to the warrant requirement.[148] Although other exceptions to the warrant requirement may apply, three exceptions in particular seem most applicable if the government is seeking to obtain and use CSLI; these exceptions are exigent circumstances for hot pursuit, exigent circumstances for public safety, and the "arrest warrant exception." Each of these exceptions is discussed in turn.

A. Exigent Circumstances—Hot Pursuit

The first of these applicable exceptions allows for the police to make warrantless entries when they are in "hot pursuit" (sometimes referred to as "fresh pursuit") of a

143. *Tracey*, 152 So. 3d at 528 (Canady, J., dissenting).

144. *See supra* Part II.B for a general discussion of the differing court opinions on whether and when a warrant is required for both historical and real-time CSLI.

145. *See, e.g.*, *Tracey*, 152 So. 3d at 526 ("Because probable cause did not support the search in this case, and no warrant based on probable cause authorized the use of Tracey's real time cell site location information to track him, the evidence obtained as a result of that search was subject to suppression.").

146. *See Jones II*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (noting 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[]").

147. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that a warrant is required before a search of a cell phone incident to arrest, despite the fact that a person and his effects have been generally held to be subject to search incident to arrest).

148. *Id.* at 2482.

criminal suspect. In *Warden, Md. Penitentiary v. Hayden*,[149] the Court considered the validity of the government's warrantless search of a home. After Hayden committed a robbery, he was seen and followed to his house by witnesses, and after the police were notified they proceeded to Hayden's house, arriving "within minutes" of learning he was there.[150] The police entered the house and began searching for Hayden; along with him, they found evidence of Hayden's crime inside of the residence.[151] Here, the Court held that the warrantless entry into Hayden's home and the warrantless search for Hayden himself were both valid because the Fourth Amendment does not require law enforcement officials to delay their investigation if doing so puts them or the public in danger.[152] Although the majority opinion did not explicitly say so, Justice Fortas's concurring opinion recognized the majority's decision was authorizing government searches "in the course of 'hot pursuit.'"[153]

In *United States v. Santana*, police established probable cause to arrest a woman for a drug offense after conducting an undercover drug transaction.[154] When the police arrived at the woman's house, they saw her standing in the doorway to the home; however, upon realizing the police were present, the woman retreated into her residence.[155] The police immediately followed her, entering the woman's home in the process, and arrested her.[156] Recognizing this as a case of "true 'hot pursuit,'" the Court held that the warrantless entry into the woman's home was governed by *Hayden* and was thus valid.[157]

Hayden and *Santana* stand for the proposition that the police may enter a home, the most sacred of premises, without a warrant when they are in hot pursuit of a criminal suspect (against whom they have established probable cause to arrest), and the delay of obtaining a warrant would endanger their lives or the lives of others and lead to the escape of the perpetrator[158] or allow for the destruction of evidence.[159] This is easily applied in the context of CSLI by simply substituting the user's cell phone for his home; this would allow the government to obtain CSLI from a cell provider without a warrant when it has probable cause to believe that evidence of a crime will be found at the location to be searched, and the delay of obtaining a warrant[160] would put lives at risk, lead to the destruction of evidence, or lead to the

149. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 295–96 (1967).
150. *Id.* at 297.
151. *Id.* at 298.
152. *Id.* at 298–99.
153. *Id.* at 310 (Fortas, J., concurring).
154. United States v. Santana, 427 U.S. 38, 39–40 (1976).
155. *Id.* at 40.
156. *Id.*
157. *Id.* at 42–43.
158. *See Hayden*, 387 U.S. at 299 (defining the scope of the warrantless entry and search justified during hot pursuit to be as broad as necessary in order to prevent resistance or escape by the suspect).
159. *See Santana*, 427 U.S. at 43 (holding the warrantless entry into a home justified during hot pursuit because there was "a realistic expectation that any delay would result in destruction of evidence").
160. One district court noted that, on the facts presented in the case, obtaining a warrant for CSLI could take approximately six hours, notwithstanding the "several days or weeks thereafter before the cell phone location data would be provided by the cellular service provider." United States v. Caraballo, 963 F. Supp. 2d 341, 363 (D. Vt. 2013). Under these circumstances, the requirement that there be a significant delay appears to be met as a matter of

escape of the cell phone user suspected of the crime.[161] In fact, several lower courts have applied this exception to CSLI cases with results that are consistent with the requirements of the Fourth Amendment.

In *State v. Subdiaz-Osorio*, officers were investigating the stabbing death of a man that had occurred early one morning.[162] Just before noon on the same day, the police learned that the suspect had borrowed a vehicle and may have been seeking to leave the state—possibly even the country.[163] Some time after noon on the same day, the police sought to track the suspect's cell phone, submitting a request to the cell service provider outlining the exigent circumstances present; specifically, that they were looking for a homicide suspect who was "armed and dangerous" and may be looking to "flee the state or the country to avoid prosecution."[164] Later in the afternoon, law enforcement was able to obtain the tracking information for the suspect, which placed him in Arkansas (three states away).[165] The suspect's vehicle information was given to the police in Arkansas around 5:43 p.m., and the suspect was located and taken into custody around 6:11 p.m.—or approximately twenty-eight minutes later.[166] Assuming for the sake of argument that obtaining CSLI from the suspect's phone was a search, the Wisconsin Supreme Court held that this search would not violate the Fourth Amendment because it fell within the exigent circumstances exception to the warrant requirement.[167] In fact, the police in this case "had their pick of three exigent circumstances"—the threat to the safety of others, the risk that the suspect would destroy evidence, and the likelihood that the suspect would flee the country.[168]

The *Subdiaz-Osorio* case met the requirements of exigent circumstances while in hot pursuit because, although the crime itself happened much earlier in the morning, the police were actively investigating the crime as soon as they were informed of it and they acted on the information they had without delay, including submitting the request to the cell service provider shortly after obtaining the suspect's cell phone number.[169] Further, there was sufficient evidence from which

course when attempting to obtain CSLI from a cell service provider. *See id.* (noting that after several days or weeks, the data might have forensic value but could not be used to remedy the exigent circumstances presented).

161. *See generally* State v. Subdiaz-Osorio, 849 N.W.2d 748, 770 (Wis. 2014) (requiring the government to establish probable cause that evidence will be found at the location to be searched, and that there are exigent circumstances in the form of threats to safety, risk of losing evidence, and likelihood that suspect will flee).

162. *Id.* at 754.

163. *Id.* at 754–55.

164. *Id.* at 756.

165. *Id.* at 757.

166. *Id.* at 757.

167. *Subdiaz-Osorio*, 849 N.W.2d at 768.

168. *Id.* at 770.

169. *Id.* at 756–58. Exact times are not given, but the factual background indicates that the witness who provided the suspect's cell phone number was interviewed from "around 10 a.m. . . . until about 12 p.m." and that the police began seeking CSLI from the suspect's phone "[s]ometime after 12 p.m." *Id.* at 754–55. This suggests that the police could have began seeking CSLI within the span of a few minutes, but also that it could have taken over two hours for the police to act on the information received from the witness. Interestingly, the police obtained a search warrant to search the suspect's home, and a detective indicated that authoring a search warrant and having it signed by a judge "usually takes between two and three hours." *Id.* at 756. On these facts, it is at least possible that the police could have obtained a search warrant to get the suspect's CSLI if they received his cell phone

the police could establish probable cause to search the suspect's phone to obtain evidence of the murder and support a finding that exigent circumstances existed and that a delay would jeopardize lives, potential evidence, and the successful apprehension of the suspect.[170]

Although it may seem easy to establish exigent circumstances, the courts have not accepted all assertions of exigent circumstances by law enforcement in the context of CSLI. For example, in *Herring v. State*, the court noted that there was at least some justification for a finding of exigent circumstances, since Herring may have been armed and that a delay in his apprehension could jeopardize the lives of other officers as well as those of the public.[171] However, the police obtained Herring's cell phone information at 11:15 p.m. and the police did not contact the cell phone provider to obtain CSLI for Herring's phone until 1:52 a.m. the next day—a delay of over two-and-a-half hours.[172] This large gap of time, coupled with no explanation as to why officers could not have obtained a search warrant during this delay, was enough to defeat a finding of exigent circumstances.[173]

In keeping with these cases, in order to obtain admissible evidence when they seek to act under exigent circumstances in hot pursuit, the police should act on the information they receive regarding a suspect's cell phone without unreasonable delay; any delays in acting on this information should be well documented to support the necessary assertion that there was no time to obtain a CSLI search warrant.[174] In addition, the police should indicate how long it usually takes to draft a warrant for CSLI, to have that warrant signed, to serve it on a cell service provider, and to have the provider respond with that information; this information could be crucial to a decision on whether exigent circumstances existed.[175] Finally, the police must be able to establish that a delay in obtaining CSLI from a cell service provider would either jeopardize their safety or the safety of another person, create a risk of the destruction of evidence of the crime that they are investigating, or allow the suspect to evade apprehension; this could be as simple as providing facts supporting an assertion that the suspect may be armed and dangerous, is suspected of a crime of violence, may still be in possession of evidence of the crime, and could be seeking

information at the start of the witness interview; however, this does not take into account the response time of the cell service provider.

170. *See Subdiaz-Osorio*, 849 N.W.2d at 770.

171. Herring v. State, 168 So. 3d 240, 243 (Fla. Dist. Ct. App. 2015).

172. *Id.* at 242.

173. *Id.* at 244 (explaining that "the State failed to present testimony to establish that officers could not have obtained a warrant during the 2.5 hour period at issue"). As noted previously, it could take several hours simply to draft the search warrant to obtain CSLI, and then several days or weeks to get a response. United States v. Caraballo, 963 F. Supp. 2d 341, 363 (D. Vt. 2013). Thus, the problem may not necessarily have been with the amount of time that passed before law enforcement conducted the search, but rather the fact that no information was presented to justify the amount of time that passed between obtaining Herring's cell phone information and actually conducting the search.

174. *See Herring*, 168 So. 3d at 244 (quoting Hornblower v. State, 351 So. 2d 716, 718 (Fla. 1977)) ("[I]f time to get a warrant exists, the enforcement agency must use that time to obtain a warrant.").

175. *Compare Caraballo*, 963 F. Supp. 2d at 363 (holding that exigent circumstances existed, relying in part on the fact that it could take weeks to complete the warrant process) *with Herring*, 168 So. 3d at 244 (holding that exigent circumstances did not exist because officers did not attempt to obtain warrant and did not explain why they could not obtain a warrant in two-and-a-half hours).

to flee the jurisdiction.[176] Complying with these requirements, the police should be able to successfully obtain and use CSLI and avoid suppression of the resulting evidence at trial.

B. Exigent Circumstances—Public Safety

The next applicable exception—exigent circumstances for concern of public safety[177]—is a close cousin of the exception surrounding hot pursuit. However, it is distinct in that, while the hot pursuit doctrine requires the police to establish probable cause for a crime, among other requirements,[178] the public safety doctrine requires only that the police "have an objectively reasonable basis for believing that an occupant is seriously injured or imminently threatened with such injury."[179] This rule was announced in *Brigham City, Utah v. Stuart*, where the Court considered the warrantless entry into a residence during a police response to a loud party.[180] After officers arrived at the residence, they heard an altercation occurring inside the residence, entered the backyard to see juveniles drinking beer there and observed what appeared to be the beginning of a fight inside the residence.[181] The police then entered the residence to quell the violence;[182] on these facts, the Court found that the officers had an objectively reasonable basis for believing an injured adult may need help and that future violence was imminent, and held that there was no Fourth Amendment violation.[183]

The Court affirmed this holding in *Michigan v. Fisher*, where officers responded to a man "going crazy" inside his own residence.[184] When the police arrived, they saw the man's vehicle and house damaged, with broken glass lying around, and blood on one of the doors to the house and on the vehicle.[185] Looking through a window, the police could see the man inside his house screaming and throwing things; the man appeared to have been injured, but refused to tell police whether he needed medical attention.[186] When the police entered the man's residence, he pointed a gun at one of the officers; he was subsequently arrested and charged with assault

176. *See* State v. Subdiaz-Osorio, 849 N.W.2d 748, 770–72 (Wis. 2014) (finding exigent circumstances to obtain CSLI when the police provided facts supporting all of these assertions); United States v. Takai, 943 F. Supp. 2d 1315, 1323 (D. Utah 2013) (finding exigent circumstances to obtain CSLI when detective had knowledge that defendant was known to be violent, believed defendant to be armed and dangerous, and reasonably believed that a robbery would be committed by the defendant in the future).

177. This is also referred to as the emergency aid exception. *See* Michigan v. Fisher, 558 U.S. 45, 47 (2009).

178. *See* United States v. Santana, 427 U.S. 38, 42–43 (1976) (approving warrantless entry when police had probable cause to arrest defendant prior to making entry into her home to arrest her, and noting that the same occurred in *Hayden*).

179. Brigham City v. Stuart, 547 U.S. 398, 400 (2006).

180. *Id.* at 406.

181. *Id.*

182. *Id.*

183. *Id.* at 406–07. Interestingly, Justice Stevens joined the unanimous opinion, but wrote separately to explain that he felt the Court's opinion simply restated "well-settled rules of federal law" and that "it [was] hard to imagine the outcome was ever in doubt[,]" so much so that he would have denied certiorari on this case. *Id.* at 407–09 (Stevens, J., concurring).

184. Michigan v. Fisher, 558 U.S. 45, 45 (2009).

185. *Id.* at 45–46.

186. *Id.* at 46.

with a deadly weapon.[187] The Court applied *Stuart* and held that law enforcement was able to invoke exigent circumstances involving public safety to make a warrantless entry into the man's home because it was reasonable to believe that he hurt himself and needed help or that he was about to hurt or had already hurt someone else.[188]

This exception is easily adapted to apply to CSLI; in fact, the Stored Communications Act specifically allows cell service providers to divulge the contents of any communication to be disclosed to any government entity "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[189] In situations where members of law enforcement are seeking CSLI, they would provide information sufficient for the cell service provider to meet the standard announced in *Stuart*, and the provider would then be able to release the information to the police.[190] Currently, there are no cases that discuss the applicability of the exigent circumstances for public safety exception in the context of CSLI—perhaps because in cases where it has been used, the parties (or the courts) have recognized that it is appropriate under both the Stored Communications Act and the seemingly common-sense notions behind the public safety exception.[191] However, real-life examples show the straightforward application of, and the necessity for, such an exception as applied to CSLI.

In one incident, the police received a phone call late one Sunday evening from a woman screaming for help and begging to be released from a vehicle; the call was abruptly cut short.[192] Acting quickly, a police dispatcher contacted the woman's cell service provider and obtained the name of the phone's owner, as well as the location of the phone.[193] Using this location information, as well as other information obtained from conducting research on the phone's owner, allowed police to locate the victim "within moments" and rescue her from her kidnapper.[194] Simply having someone asking for help and wanting to get out of a vehicle may provide some suspicion that criminal activity is at hand, but likely falls short of the probable cause required for the exigent circumstances in hot pursuit exception.[195] Further, based solely on that brief contact, it would be hard to say with certainty that the incident

187. *Id.*

188. *Id.* at 49.

189. 18 U.S.C. § 2702(b)(8) (2012). The same law also allows for subscriber information to be obtained under the same circumstances. § 2702(c)(4). States have also enacted statutes that allow for the same disclosures under similar circumstances. *See, e.g.*, FLA. STAT. §§ 934.22(2)(f), (3)(a) (2015).

190. Past cases suggest that the cell provider would receive the information from law enforcement via a faxed form on which the police certify facts that justify a claim of exigent circumstances, and thereafter would provide the requested information to law enforcement. *See* State v. Subdiaz-Osorio, 849 N.W.2d 748, 756 (Wis. 2014); United States v. Caraballo, 963 F. Supp. 2d 341, 345–47 (D. Vt. 2013).

191. *See* Brigham City v. Stuart, 547 U.S. 398, 407–09 (2006) (Stevens, J., concurring).

192. Julie Manganis, *Police Credit Dispatcher with Locating Kidnap Victim*, SALEM NEWS (May 20, 2014), http://www.salemnews.com/news/local_news/police-credit-dispatcher-with-locating-kidnapvictimarticle_464b9723-8160-5804-bead-331cd218bf93.html.

193. *Id.*

194. *Id.*

195. *See supra* Part III.A for a discussion of the requirements of the exception for exigent circumstances while the police are in hot pursuit of a suspect.

involved "danger of death or serious physical injury" as required under the Stored Communications Act, at least if the language of the statute is construed strictly.[196] However, under the public safety exception, a person calling 911 and screaming for help would seem at least as serious as a man who had a "cut on his hand" but was refusing to communicate with police.[197] And since the exception does not require "ironclad proof of 'a likely serious, life-threatening' injury" but instead only "'an objectively reasonable basis for believing' that medical assistance was needed[] or persons were in danger," it would certainly cover the scenario described above.[198] Clearly then, the exception for exigent circumstances for public safety, as applied to CSLI, has its place as a useful tool for allowing law enforcement to safeguard lives in a broad range of emergency situations.[199]

In order to make use of this exception, members of law enforcement should carefully document the facts and circumstances that lead them to believe there is someone who is in need of medical assistance or is in legitimate danger of serious injury.[200] In the context of obtaining CSLI, this would most likely come from the contents of a cell phone call to a 911 operator from a person in distress (like the example above), a report from family members or close friends about a missing and endangered loved one, or some similar situation. Once obtained and documented, this information should be immediately reported to a cell service provider, who can then provide the police with the location information necessary to locate and assist the citizen in need.[201] Complying with these requirements, law enforcement should be able to avoid any Fourth Amendment violations.

C. The "Arrest Warrant Exception"

Although not as straightforward as the public safety exception, the "arrest warrant exception" is an equally valuable tool that would allow the police to safeguard the public by locating and apprehending wanted criminals. Born in *Payton*, this exception allows an officer armed with an arrest warrant "to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within."[202] Applying this to CSLI, one might present a rule that would allow the police to obtain CSLI for the subject of an arrest warrant, since the entry into a suspect's home is

196. §§ 2702(b)(8), (c)(4).
197. Michigan v. Fisher, 558 U.S. 45, 46 (2009).
198. *Id.* at 49.
199. It does not appear that any case has interpreted whether the requirement that there be a "danger of death or serious physical injury," §§ 2702(b)(8), (c)(4), has the same meaning as a requirement for "an objectively reasonable basis for believing that [someone] is seriously injured or imminently threatened with such injury," Brigham City v. Stuart, 547 U.S. 398, 400 (2006). However, if the statute were to be interpreted to require the same proof as that required in *Stuart*, then admittedly there would be no need for a public safety exception for CSLI, except perhaps that the exception would allow the police to demand or seize the information whereas the statute allows service providers to voluntarily disclose the information (and thus they could choose not to do so).
200. This would comply with the requirements of *Fisher*, 558 U.S. at 49.
201. Because this exception relies on exigent circumstances, it is important that officers avoid any unnecessary delays; if there is an unreasonable and unexplainable delay, the police risk violating the cell phone user's Fourth Amendment rights. *See, e.g.*, Herring v. State, 168 So. 3d 240, 244 (Fla. Dist. Ct. App. 2015).
202. Payton v. New York, 445 U.S. 573, 603 (1980).

instead replaced with entry into the suspect's cell phone.[203] At first glance, this might make sense because the previous two exceptions were adapted to allow the police to obtain CSLI by the same substitution. However, close inspection of the rule in *Payton* reveals a problem: unlike the rules based on exigent circumstances, the "arrest warrant exception" only allows the police to enter the *suspect's* home.[204] Clearly then, applying *Payton* to CSLI presents a problem that it also presents in its original form—namely, what happens if the police track a suspect into a residence that is not his or her own?[205]

In *Steagald v. United States*, the Court confronted this problem when the DEA sought to arrest a federal fugitive wanted for drug law violations.[206] Believing that the fugitive was within a particular residence, the police entered the residence and discovered drugs inside; the person to be arrested was not there, nor did he live there.[207] Thus, the police had entered the home of a third party searching for the subject of the arrest warrant. In rejecting the idea that the arrest warrant previously issued was sufficient to justify the entry into the residence, the Court pointed out that the arrest warrant satisfied the Fourth Amendment rights of the person to be arrested, but not the rights of the third-party residents.[208] If an arrest warrant could be used as the authority to enter the homes of third parties, it would effectively convert an arrest warrant—naming only the individual to be seized—into a general warrant, and clearly this is an undesirable result.[209] Accordingly, in order to enter the residence of a third party, the Court held that the police must obtain a search warrant for the residence they wish to enter.[210]

Requiring a search warrant to be issued based on the arrest warrant would defeat the purpose of a warrant exception, yet the issue created by *Steagald* must be dealt with in order to craft a valid exception that does not violate the Fourth Amendment rights of third parties. In considering an appropriate adaptation of the rule in *Payton*, it is important to note that obtaining and monitoring CSLI "is, of course, less intrusive" from an actual physical entry into a third-party residence; however, this

203. The argument in this section assumes that the police have established, at least to the required burden of proof, that the subject of the arrest warrant has a cell phone and also have the number for the phone.

204. *Id.* ("[F]or Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling *in which the suspect lives* when there is reason to believe the suspect is within") (emphasis added).

205. Even if the police tracked a suspect into a third-party residence, unless the suspect has standing to object to a search of the residence, the evidence obtained in the form of tracking will still be admissible against that suspect. *See* United States v. Karo, 468 U.S. 705, 719–20 (1984). This naturally means that if the police conduct electronic surveillance inside of a home but do not obtain evidence that is used against a party with standing, there can be no suppression of evidence. Certainly, anyone whose home is invaded by electronic surveillance could raise a claim against the government for a violation of his or her constitutional rights. *See* 42 U.S.C. § 1983 (2012). Because of this, despite what may be a situation in which the aggrieved party would receive only nominal damages due to the minimal harm associated with a non-physical intrusion into the home, this Note will seek to craft a rule that will avoid all Fourth Amendment violations, and not just violations that would result in the suppression of evidence.

206. Steagald v. United States, 451 U.S. 204, 206 (1981).

207. *Id.* at 206–07.

208. *Id.* at 216.

209. *Id.* at 220.

210. *Id.* at 222.

fact alone will not justify the rule to be created here.[211] This is because the government violates the Fourth Amendment when it seeks to

> determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—*or a person, for that matter*—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.[212]

Given this, the Court would almost certainly hold that the mere fact the police are not making actual entry into a third-party residence, and instead just monitoring a cell phone signal, to determine the presence of a cell phone's user is not enough to justify the "arrest warrant exception." But a close examination of *Karo* may provide the solution for the proper formulation of this exception. Although the Court in *Karo* held that monitoring of the beeper while inside of a private residence was a search,[213] when they examined the monitoring of a beeper inside of a locker rented by two of the defendants, the Court held there was no Fourth Amendment violation because the beeper did not identify the specific locker that had the ether and revealed nothing about the contents of the locker.[214] In fact, the police only identified which locker contained the ether when they walked in public areas of the facility and used their ordinary sense of smell to determine which locker contained the ether.[215]

Using this holding allows the "arrest warrant exception" to justify obtaining CSLI despite the potential invasion of privacy to third parties. First, in obtaining either historical or real-time CSLI under this "exception," the information obtained is exactly the same;[216] while in limited circumstances this information could approach GPS-like precision,[217] in most cases, law enforcement officials will receive information regarding which cell tower the user is or was connected to, and which sector of the cell phone tower the user was covered by.[218] Thus, just like in *Karo*, the

211. *See* United States v. Karo, 468 U.S. 705, 715 (1984) (even though monitoring a beeper is not the same as a full-scale search, it reveals information about the interior of the home that the police could not have obtained without a warrant).
212. *Id.* at 716 (emphasis added).
213. *Id.* at 714.
214. *Id.* at 720.
215. *Id.* at 720–21.
216. *Jones I*, 908 F. Supp. 2d 203, 207 (D.C. Cir. 2012).
217. CDT, *supra* note 30, at 4.
218. United States v. Davis, 785 F.3d 498, 515 (11th Cir. 2015). Moreover, in executing several search warrants to obtain both historical and real-time CSLI, the author has made several important observations. First, historical CSLI has, in every instance, only provided the location of the cell phone tower to which the cell phone was connected, and the sector that covered the location of the cell phone. Second, while "pinging" a phone and obtaining real-time CSLI can provide more accurate location information than its historical counterpart, it often lacks the precision of a GPS unit; the typical "location" of the phone covers three houses in a residential neighborhood and, despite what one may assume, the phone is not always located in the "middle" house, making finding the phone a shell game of sorts. Further, in urban areas, even near-GPS accuracy was not conclusive as to location, since these areas can contain duplexes, attached townhomes, and apartment complex buildings, just to

police will know the general area in which to search, but will likely not know precisely in which home (if any) the user currently resides, and they will have to use other legal methods to determine the precise location of the cell phone user. Since the CSLI obtained will reveal nothing about the inside of any home, like the lockers in *Karo*, the issues presented in *Steagald* are safely avoided.[219] Further, when applying *Wyoming v. Houghton* and balancing the intrusion on individual privacy with the need to promote legitimate governmental interests,[220] the "arrest warrant exception" proposed is reasonable. There is minimal intrusion on individual privacy because only the general location of the user's phone is conveyed to law enforcement, there is judicial oversight to ensure there are no arbitrary invasions of privacy because a judge will have to first issue the arrest warrant in order for the police to make use of this exception, government action that complies with the law is presumed reasonable, and the information sought serves the compelling governmental interest of apprehending a wanted fugitive.[221]

Although no case has yet to examine the use of the "arrest warrant exception" for CSLI,[222] this too would be a relatively straightforward act. The police would provide a copy of the warrant, along with the suspect's cell phone information, to the cell service provider, and the provider would then relay the CSLI to law enforcement as needed until the suspect is apprehended.[223] Based on the holding in *Payton* and the other cases discussed, this should allow the police to avoid any Fourth Amendment violations. However, as a practical matter, this exception may never be tested. If the police have taken the time to obtain an arrest warrant for a criminal suspect, the same facts would likely support them obtaining a search warrant for the suspect's CSLI, be it historical or real-time, in order to aid in the suspect's apprehension.[224] Further, obtaining a search warrant would allow the government to avoid the problems posed by improvements in technology, since the search warrant would likely satisfy the requirements of the Fourth Amendment as to any involved

name a few multi-unit housing structures; plain observations and additional resources were needed to narrow down the exact location of the phone.

219. Despite this, the "arrest warrant exception" may not survive long based on this justification; as technology continues to improve, the accuracy of locating a user's cell phone may also improve to the point that the police will be able to narrow a suspect's presence down to the interior of a residence. *See, e.g.*, *Hearing*, *supra* note 25, at 26. When this happens, the government will move from *Karo*'s locker scenario to the scenario of its more famous holding—the monitoring of the interior of a home. *Karo*, 468 U.S. at 715. At that point, *Steagald* again becomes an issue that must be dealt with if the government seeks to use this "exception."

220. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

221. *See supra* Part II.A for a full discussion of all these factors in the context of historical CSLI; they are equally applicable in the analysis of this "exception," since the factors are used to test the reasonableness of government action in light of the Fourth Amendment. *See also* Rothstein, *supra* note 22, at 533 ("Tracking used exclusively to facilitate arrest is reasonable.").

222. There is at least one case that discussed using CSLI in the context of facilitating arrest; specifically, United States v. Bermudez, No. IP05-0043-CR05-BF, 2006 WL 3197181, at *4–40 (S.D. Ind. June 30, 2006) *aff'd sub nom.* United States v. Amaral-Estrada, 509 F.3d 820, 829 (7th Cir. 2007). However, in this case, the CSLI was obtained pursuant to a court order, thus it is not directly applicable to the analysis of the "arrest warrant exception" contemplated here. *Id.* at *1.

223. This is similar to the process used in the exigent circumstances cases. *See* State v. Subdiaz-Osorio, 849 N.W.2d 748, 756 (Wis. 2014); United States v. Caraballo, 963 F. Supp. 2d 341, 345–47 (D. Vt. 2013).

224. In fact, the author, in his capacity as a detective with over a decade of law enforcement experience, has used exactly the same facts provided in an arrest warrant to obtain a search warrant for both a suspect's historical and real-time CSLI on several occasions.

third parties.[225] Thus, while the "arrest warrant exception" could likely pass constitutional muster, as a practical matter its employment is unlikely.

CONCLUSION

Cell phones are an integral part of American life; in fact, many people forego obtaining a traditional telephone line in their home in favor of having solely a cell phone.[226] Given the cell phone's pervasive presence in American society, concern that these "lifelines" are not turned into tracking devices on a government whim is a legitimate concern. At the same time, completely denying the police the ability to use this tool to accomplish the legitimate purpose of law enforcement is undesirable. Thankfully, current law allows law enforcement officials to get this information with a court order, albeit on a standard below probable cause—and that is the crux of the current issue in the courts revolving around CSLI. Kendrick Herring was not the first person to be tracked using his cell phone information, but his case and the many other cases involving CSLI have been decided in a mire of case law surrounding the topic. Where some jurisdictions allow the police to obtain CSLI based solely on a court order, other jurisdictions demand a warrant; where some jurisdictions hold CSLI to be an invasion of privacy depending on whether real-time or historical CSLI is sought, others hold that CSLI should be treated the same regardless of what the government is seeking.

Despite diverging opinions on the topic, one thing is certain; although the Supreme Court has not ruled directly on the issue, relevant and binding case law from the Court supports the ability of the police to obtain CSLI without a warrant. The third-party doctrine created in *Miller* and applied to electronic surveillance in *Smith* clearly supports the assertion that the government only needs to obtain a court order in order to obtain CSLI in either of its forms. Simply put, CSLI is information generated and maintained by cell service providers as a business record, and this fact is widely known by cell phone users, who cannot maintain a realistic expectation of privacy in those records. So long as this doctrine exists in its current form, no warrant is required when the government seeks to obtain and use this information against a criminal defendant, and courts should deny motions to suppress evidence obtained alleging Fourth Amendment violations on this ground.

While the third-party doctrine clearly controls the distribution of CSLI to law enforcement, the Court's modification of this doctrine is not completely out of the question; in fact, it was plainly suggested in Justice Sotomayor's concurrence in *Jones*, and other courts have ruled that a warrant is required for CSLI because the third-party doctrine is inapplicable. However, even if a warrant is required, the government can still obtain this information under three different exceptions to the warrant requirement. If members of law enforcement are in hot pursuit of a criminal suspect and quickly seek CSLI from the cell service provider, they can use the exception to the warrant requirement for exigent circumstances. Further, if the police

225. Rothstein, *supra* note 22, at 526.

226. During the study conducted by the Pew Research Center, over half of the people interviewed over a cell phone did not have a landline telephone. *See* ANDERSON, *supra* note 7, at 16.

are attempting to render emergency aid to a 911 caller whose call is suddenly disconnected, they can use the same exception to the warrant requirement on the basis of public safety. Finally, although somewhat impractical, the government may be able to use the "arrest warrant exception" outlined in *Payton* in order to obtain CSLI for the subject of an arrest warrant. Thus, regardless of the final decision regarding a warrant requirement for CSLI, law enforcement should still be able to obtain this information in a timely fashion without a warrant when it is urgently needed.

Given the value of this tool and the varying decisions in different jurisdictions, a decision from the Court is needed in order to decide, once and for all, the rules for using it. It is true that the law frequently lags behind technological advances, but cell phone technology has been available for quite some time, and decisions regarding this problem have been sprouting up for at least a decade. Every moment without firm guidance potentially leads to the loss of vital evidence in a criminal case—or worse, the opportunity to safeguard a life. However, a decision from the Supreme Court will give the police a firm guidepost, regardless of whether the Court chooses to require a warrant, and will make stable at least one small aspect of the constantly changing legal landscape that they must navigate each day.