Nova Law Review

Volume 39, *Issue* 2 2017 *Article* 3

Why The Eleventh Circuit Got It Wrong: Historical Cell Site Location Information Is Not Considered A Search Within The Meaning Of The Fourth Amendment

Stephanie H. Carlton*

*

Why The Eleventh Circuit Got It Wrong: Historical Cell Site Location Information Is Not Considered A Search Within The Meaning Of The Fourth Amendment

Stephanie H. Carlton

Abstract

On August 7, 2010, three men brandishing guns entered a pizzeria in South Florida and demanded cash from an employee.

KEYWORDS: real-time, opinion, wrong

WHY THE ELEVENTH CIRCUIT GOT IT WRONG: HISTORICAL CELL SITE LOCATION INFORMATION IS NOT CONSIDERED A SEARCH WITHIN THE MEANING OF THE FOURTH AMENDMENT

STEPHANIE H. CARLTON*

I. INTRODUCTION 239
II. FOURTH AMENDMENT OVERVIEW 241
A. *What Constitutes a Search?* 242
III. FOURTH AMENDMENT AND CELL PHONE TECHNOLOGY 243
A. *Cell Site Location Information ("CSLI")* 243
1. Historical Versus Real-Time Location Information 244
a. *The Stored Communications Act* 245
b. *Third Circuit Opinion* 247
IV. UNITED STATES V. DAVIS: WHY THE ELEVENTH CIRCUIT GOT IT WRONG 249
A. *No Reasonable Expectation of Privacy: Third Party Doctrine* 249
B. *Historical CSLI: A Voluntary Disclosure to a Third Party* 252
1. Comparison to *United States v. Davis* 253
C. *The Beeper Cases* 254
1. CSLI Differs from Beeper Cases 257
D. United States v. Jones 258
1. Why *Jones* Analysis Does Not Apply 259
E. Katz *Analysis Applied to* Davis 261
V. CONCLUSION 262

I. INTRODUCTION

On August 7, 2010, three men brandishing guns entered a pizzeria in South Florida and demanded cash from an employee.[1] About a month later,

* Stephanie Carlton is a J.D. candidate for May 2016 at Nova Southeastern University, Shepard Broad College of Law. Stephanie would like to extend a thank you to her colleagues at the *Nova Law Review* for their hard work to improve and refine this article. She would also like to thank her mother and father who have endlessly supported her throughout her law school journey.

the same group ran into a car parts store and forced an employee at gunpoint to unlock the safe.[2] When the employee scrambled to open the safe, the armed men screamed in the employee's face, threatening to kill him.[3] "Eventually, when the safe did not open, [the robbers] fled."[4] As he fled with his accomplices, Davis shot at a dog that was merely barking at them.[5]

The group of robbers, in a two-month span, terrorized the South Florida community by committing a series of seven armed robberies.[6] Eventually, surveillance video, DNA, and cell site location information ("CSLI") enabled the police to catch the violent group.[7] Notably, "[h]istorical [CSLI] showed that Davis and his accomplices had placed and received cell phone calls in close proximity to the locations of the crimes around the times that the crimes were committed."[8] Obtaining historical CSLI, and the use of it as evidence during Davis's trial, became a controversial issue during Davis's appeal.[9] The governmental obtainment of historical CSLI with a court order rather than a warrant has created a Fourth Amendment debate.[10] Should the government be required to demonstrate probable cause to secure a warrant to obtain historical CSLI?11 Although this modern constitutional debate has been considered in other circuits, *United States v. Davis*[12] raises an issue of first impression in the Eleventh Circuit Court of Appeals.[13]

This Comment analyzes the prevailing controversy surrounding technology, government, and privacy.[14] It begins by exploring the elements of the Fourth Amendment and the predominant cases dealing with privacy such as *Katz v. United States*.[15] Part two discusses what constitutes a search under the Fourth Amendment and presages the discussion of why obtaining

1. Brief for the United States at 5, United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (No. 12-12928-EE).
2. *Id.* at 6–7.
3. *Id.* at 7.
4. *Id.*
5. *Id.*
6. *See* Brief for the United States, *supra* note 1, at 4–9.
7. *See id.* at 9–10.
8. *Id.* at 10.
9. *See* United States v. Davis, 754 F.3d 1205, 1211 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014).
10. *See id.*
11. *See id.*
12. 754 F.3d 1205 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014).
13. *Id.* at 1210.
14. *See infra* Parts II–V.
15. 389 U.S. 347 (1967); *see infra* Part II.

historical CSLI does not constitute a search that will be discussed in the latter part of the Comment.[16]

Part three of this Comment discusses historical CSLI and this non-invasive law enforcement practice.[17] This section elaborates on the difference between historical and real-time CSLI while explaining why historical CSLI is non-invasive and does not constitute a search within the meaning of the Fourth Amendment.[18]

Part four—the largest and most significant part—focuses on the recent Eleventh Circuit decision of *Davis*.[19] This section contains an in-depth critique of the opinion.[20] Additionally, it explains the mistake the Eleventh Circuit made in comparing the case at hand to *United States v. Jones*.[21] This Part then discusses other weaknesses of the opinion and explains how and why the court's decision was misguided.[22]

The purpose of this Comment is to educate the public on the misinterpretation of the Fourth Amendment and to explain why one does not have an expectation of privacy in public.[23] Lastly, this Comment analyzes the recent Eleventh Circuit decision and discusses why the court got it wrong when it comes to Fourth Amendment implications and historical CSLI.[24]

II. FOURTH AMENDMENT OVERVIEW

The Fourth Amendment of the United States Constitution warrants "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[25] The Fourth Amendment is designed to protect the privacy of individuals from unlawful intrusion by the government.[26] An individual must have a "'constitutionally protected reasonable expectation of privacy'" in order to obtain protection

16. *See infra* Part II.A.
17. *See infra* Part III.
18. *See infra* Part III.
19. United States v. Davis, 754 F.3d 1205, 1223 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014); *see infra* Part IV.
20. *See infra* Part IV.
21. No. 10-1259, slip op. 1 (U.S. Jan. 23, 2012); *see infra* Part IV.
22. *See infra* Part IV.
23. *See* United States v. Shanks, 97 F.3d 977, 980 (7th Cir. 1996) (finding defendant lacked legitimate expectation of privacy when he left garbage bags filled with contraband next to the street).
24. *See infra* Parts II–IV.
25. U.S. CONST. amend. IV.
26. Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 712 (2012).

under the Fourth Amendment from an unreasonable search or seizure.[27] To determine whether an individual's expectation of privacy is reasonable the Court in *Katz* developed a two-part test.[28] The first part of the test involves whether "the individual manifested a subjective expectation of privacy in the object of the challenged search."[29] The second part of the test asks whether "society [is] willing to recognize that expectation as reasonable."[30] The reasonable expectation of privacy, however, does not extend to what an individual consciously reveals to the public.[31] Furthermore, the expectation of privacy, construed from the Fourth Amendment, is determined by the context of each case.[32]

A. *What Constitutes a Search?*

To determine whether the government has performed an unreasonable search protected under the Fourth Amendment, one must determine whether that person exhibits an actual or subjective expectation of privacy which society is ready to accept as reasonable.[33] If no expectation of privacy exists then a search without a warrant does not violate the Fourth Amendment.[34] If, however, a person does have a reasonable expectation of privacy, the government cannot seize evidence without a warrant supported by probable cause.[35]

A person does not have a subjective expectation of privacy to what he or she exposes to the public.[36] When "a person knowingly exposes [information] to the public," he or she can no longer subjectively believe that information will be kept private, and therefore will not benefit from Fourth Amendment protections.[37]

27. California v. Ciraolo, 476 U.S. 207, 211 (1986) (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).
28. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
29. *Ciraolo*, 476 U.S. at 211; *see also Katz*, 389 U.S. at 361 (Harlan, J., concurring).
30. *Ciraolo*, 476 U.S. at 211; *see also Katz*, 389 U.S. at 361 (Harlan, J., concurring).
31. *Katz*, 389 U.S. at 351.
32. Malone, *supra* note 26, at 712.
33. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
34. *See id.*
35. *See* U.S. CONST. amend. IV.
36. *See* United States v. Shanks, 97 F.3d 977, 980 (7th Cir. 1996).
37. *Katz*, 389 U.S. at 351.

III. FOURTH AMENDMENT AND CELL PHONE TECHNOLOGY

There are roughly three hundred million cell phone subscribers in the United States alone.[38] Notwithstanding the country's growing affinity with technology, a lack of appellant precedent exists regarding what the government can and cannot obtain from technological devices, such as cell phones.[39] It is important to understand how a cell phone works in order to evaluate the few cases available regarding CSLI and to help predict future decisions.[40]

When a person places a cell phone call, a signal is conveyed to the nearest cell tower, and eventually to the carrier's office.[41] What experts refer to as a *cell site* is the "geographical location containing the cell tower, radio transceiver, and base station controller."[42] Anytime a person receives or makes a cell phone call, the carrier stores that information.[43] It should be noted that even when a cell phone user is not placing a call, his or her location can be identified because the phone is continuously interacting with the mobile network.[44] According to many scholars, due to the sophistication of mobile devices, CSLI can be obtained within a few hundred feet.[45]

A. *Cell Site Location Information ("CSLI")*

What is typically referred to as CSLI has become a widely used method for the government to help fight crime.[46] Although it has recently been used to combat criminal activity, many fear that obtainment of this information infringes on a person's Fourth Amendment rights.[47] Courts frequently differentiate between historical CSLI and real-time CSLI, also

38. *See* CTIA-THE WIRELESS ASS'N, *CTIA'S Wireless Industry Survey Results*, (2013), http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

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

40. *See* United States v. Davis, 754 F.3d 1205, 1210 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014) (stating that "Davis's Fourth Amendment argument raises issues of first impression in this circuit, and not definitively decided elsewhere in the country"); Malone, *supra* note 26, at 703 (stating that "many people probably do not consider how this technology works or what information they may inadvertently be sharing with their cell phone company").

41. Malone, *supra* note 26, at 707–08.

42. Christopher Fox, Comment, *Checking In: Historic Cell Site Location Information and the Stored Communications Act*, 42 SETON HALL L. REV. 769, 773–74 (2012).

43. *See id.*

44. Malone, *supra* note 26, at 708.

45. *Id.* at 704.

46. *Id.*

47. *Id.*; *see also* U.S. CONST. amend. IV.

known as prospective CSLI.[48] This distinction between real-time and historical CSLI is vital in the evaluation and response to privacy issues.[49] Courts have yet to sufficiently address whether CSLI deserves any constitutional protection at all.[50] The major issue facing CSLI among legal scholars is whether a warrant should be required to obtain historical CSLI.[51] Before one can obtain a warrant, probable cause must be established.[52] Even before one can delve into this complex constitutional issue, two questions must be answered.[53] The first question is whether collecting CSLI is considered a search; if it is considered a search, then there must be compliance with the Fourth Amendment.[54] Second, if obtaining CSLI is not considered a search, then what standard must the government meet in order to obtain historical CSLI?[55]

1. Historical Versus Real-Time Location Information

Historical CSLI records are obtained from a past date in time and only provide "the date, time, and duration of calls, whether calls are inbound or outbound, and show the originating and terminating cell sites for calls received or placed on the phone."[56] Cell phone carriers retain this information for a given amount of time for business purposes.[57] Real-time CSLI permits the government in present time to track a cell phone user's whereabouts.[58] The majority of courts faced with requests for real-time CSLI consistently have held the material is considered "tracking information as defined by 18 U.S.C. § 3117, which requires a warrant—and thus a showing of probable cause—before an order for disclosure of that CSLI may

48. Malone, *supra* note 26, at 704.

49. Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE. L. REV. 1875, 1884 (2011).

50. Malone, *supra* note 26, at 704.

51. *Id.* at 704–05.

52. *See* U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . .").

53. Harkins, *supra* note 49, at 1887.

54. *Id.*

55. *Id.*

56. Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, RICH. J.L. & TECH., Fall 2011, at 1, 10.

57. Scott A. Fraser, Comment, *Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571, 579–80 (2012).

58. *See id.* at 582.

be granted."[59] The real debate, however, regarding CSLI concerns historical data, as seen in *Davis*.[60] Courts have interpreted historical CSLI to be overseen by section 201 of the Stored Communications Act.[61]

a. *The Stored Communications Act*

The Electronic Communications Privacy Act of 1986 oversees the discovery of CSLI.[62] The Electronic Communications Privacy Act encompasses the Stored Communications Act in title two and "serve[s] as the basic statutory framework within which CSLI jurisprudence has developed."[63] Congress passed the Stored Communications Act to combat privacy concerns regarding the voluntary obtainment of consumers' personal information.[64] Under the Stored Communications Act, the government cannot simply compel communication companies, specifically cell phone companies, to turn over private customer information such as telephone numbers and call logs.[65] In addition, the communication companies are similarly constricted in their ability to turn over customer information to the government.[66]

Under the Stored Communications Act, a government agency may compel a communication service provider to provide the "contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant."[67] Under section 201 of the Stored Communications Act, the government may therefore obtain the actual location of a cell phone subscriber in real time only when the government agency obtains a warrant

59. Malone, *supra* note 26, at 710; *see also* Electronic Communications Privacy Act of 1986 § 108, 18 U.S.C. § 3117 (2012).

60. United States v. Davis, 754 F.3d 1205, 1210–11 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th. Cir. 2014); Malone, *supra* note 26, at 710–11.

61. Stored Communications Privacy Act of 1986 § 201, 18 U.S.C. § 2703 (2012); *Davis*, 754 F.3d at 1210–11; *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 307–08 (3d Cir. 2010); Malone, *supra* note 26, at 710.

62. Harkins, *supra* note 49, at 1894. *See generally* Electronic Communications Privacy Act of 1986 § 101, 18 U.S.C. § 2510.

63. Harkins, *supra* note 49, at 1894; *see also* Stored Communications Act § 201.

64. *See* Harkins, *supra* note 49, at 1899.

65. Harkins, *supra* note 49 at 1896; *see also* 18 U.S.C. § 2703(a). "The SCA regulates government access to stored user account information compiled by third parties in the ordinary course of business." Harkins, *supra* note 49, at 1896.

66. Blank, *supra* note 56, at 11.

67. 18 U.S.C. § 2703(a); Malone, *supra* note 26, at 718.

pursuant to probable cause.[68] While § 2703(a) only allows the government to obtain real-time location information pursuant to a warrant, § 2703(c) permits the government to obtain historical location information.[69] To obtain historical information,

> [a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service . . . only when the governmental entity: (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure; . . . (B) obtains a court order for such disclosure; [or] . . . (D) submits a formal written request relevant to a law enforcement investigation . . . .[70]

Accordingly, the government, pursuant to § 2703(c), may obtain records of cell phone subscribers with a court order by following § 2703(d) of the codified Stored Communications Act.[71]

The Stored Communications Act, section 201, sets forth the requirements needed for a government agency to obtain a court order, which would compel a carrier to turn over the information of a subscriber.[72] This subsection of the statute allows the government to obtain the location information "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[73]

Although most scholars and courts acknowledge that "a record or other information pertaining to a subscriber"[74] refers to historical CSLI, the central dispute involves what standard should be employed by courts to

---

68. U.S. CONST. amend. IV; 18 U.S.C. § 2703(a). According to the Act, a government agency may obtain the actual location of a subscriber's communications only when the agency obtains a warrant pursuant to probable cause required by the Fourth Amendment. U.S. CONST. amend. IV; 18 U.S.C. § 2703(a).

69. U.S. CONST. amend IV; 18 U.S.C. §§ 2703(a), (c).

70. 18 U.S.C. § 2703(c)(1).

> In order for historical CSLI to be available under 18 U.S.C. § 2703(c)(1), three qualifications must be met: [F]irst, the CSP must be a provider of an electronic communication service; second, the data may not be content information as defined in 18 U.S.C. § 2510(8); and third, the data must be a "record or other information pertaining to a subscriber to or customer of" an electronic communications service.

Fraser, *supra* note 57, at 583 (quoting 18 U.S.C. § 2703(c)(1)); *see also* Electronic Communications Privacy Act of 1986 § 101, 18 U.S.C. § 2510(8) (2012).

71. 18 U.S.C. §§ 2703(c)–(d); Fraser, *supra* note 57, at 585.

72. 18 U.S.C. § 2703(d).

73. *Id.*

74. *Id.* § 2703(c)(1).

authorize disclosure of historical CSLI.[75] "Over the last several years, the prevailing view among the courts was that historical CSLI was governed by the S[tored] C[ommunications] A[ct] and thus could be obtained without a warrant pursuant to an 18 U.S.C. § 2703(d) order."[76]

Conversely, many argue that a cell phone is really a tracking device and thus outside the scope of the Stored Communications Act since a tracking device is not within its definition of what is considered an electronic communication.[77] Therefore, in order for the government to compel a carrier to provide historical CSLI of a subscriber, "the information must have been stored by [a provider of electronic communications]."[78] The Third Circuit, however, has specifically addressed this issue and determined that a cell phone is *not* considered a tracking device.[79]

b. *Third Circuit Opinion*

In its holding, the Third Circuit articulated that by its nature, CSLI is not considered a tracking device and therefore should not be held to the higher probable cause standard.[80] The Third Circuit decision was the first on the appellate level that decided "whether a court can deny a [g]overnment application under 18 U.S.C. § 2703(d) after the [g]overnment has satisfied its burden of proof under that provision."[81] The government in *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*[82] submitted a request to the magistrate judge for a court order to obtain

---

75. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 307–08 (3d Cir. 2010).

76. Malone, *supra* note 26, at 721; *see also* 18 U.S.C. § 2703(d).

77. *See* Electronic Communications Privacy Act of 1986 § 101, 18 U.S.C. § 2510(12) (2012); Malone, *supra* note 26, at 724.

78. Malone, *supra* note 26, at 724.

79. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 309, 313.

80. *Id.* at 313.

> We therefore cannot accept the MJ's conclusion that CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production.
>
> In sum, we hold that CSLI from cell phone calls is obtainable under § 2703(d) order and that such an order does not require the traditional probable cause determination. . . . The MJ erred in allowing her impressions of the general expectation of privacy of citizens to transform that standard into anything else. We also conclude that this standard is a lesser one than probable cause, a conclusion that . . . is supported by the legislative history.

Id.; *see also* 18 U.S.C. § 2703(d).

81. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 305–06.

82. 620 F.3d 304 (3d Cir. 2010).

historical CSLI.[83] The magistrate judge denied the government's request and insisted on a government showing of probable cause when obtaining CSLI.[84] The Third Circuit, however, disagreed with the magistrate's ruling and held "that CSLI from cell phone calls is obtainable under a [court] order and that such an order does not require the traditional probable cause determination."[85]

Notwithstanding the Third Circuit decision, some still believe that a cell phone is considered a tracking device when the government is attempting to obtain real-time or prospective data.[86] Although many scholars support this contention, this Comment from here on focuses solely on historical CSLI.[87]

Even though government agencies frequently use historical CSLI to investigate criminal activity throughout the country,[88] a few scholars and courts believe section 2703(d) should be discarded and replaced with a newer and higher standard of probable cause.[89] The Third Circuit, however, has held that to determine what standard a court should employ when a government agency attempts to obtain historical CSLI is not an issue for the courts to decide, and that the standard should, instead, be left up to Congress.[90]

> We respectfully suggest that if Congress intended to circumscribe the discretion it gave to magistrates under § 2703(d) then Congress, as the representative of the people, would have so provided. Congress would, of course, be aware that such a statute mandating the issuance of a § 2703(d) order without requiring probable cause and based only on the Government's word may evoke protests by cell phone users concerned about their privacy. The considerations for and against such a requirement would be for Congress to balance. A court is not the appropriate forum for

83. *Id.* at 305.

84. *Id.* at 305, 308.

85. *Id.* at 313. "We also conclude that this standard is a lesser one than probable cause, a conclusion that . . . is supported by the legislative history." *Id.*

86. Malone, *supra* note 26, at 724–25.

87. *E.g.*, *id.*, at 724–25; *see infra* Parts III–V.

88. *See* Malone, *supra* note 26, at 724.

89. *See In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 307–08 (3d Cir. 2010); Malone, *supra* note 26, 704–05.

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

> such balancing, and we decline to take a step to which Congress is silent.[91]

This precedent-setting decision offered by the Third Circuit—while one of the first federal circuit court decisions regarding historical CSLI—most likely will determine how future courts will examine the governmental obtainment of historical CSLI.[92]

IV. UNITED STATES V. DAVIS: WHY THE ELEVENTH CIRCUIT GOT IT WRONG

The next section of this Comment focuses on the misguided decision of the Eleventh Circuit in *Davis*.93 This section will provide evidence showing why the court was misguided.94

A. *No Reasonable Expectation of Privacy: Third Party Doctrine*

Although the Eleventh Circuit claims that a cell phone subscriber has a subjective expectation of privacy, this expectation of privacy may not be one that society is willing to accept as reasonable.[95] The Supreme Court has repeatedly articulated that Fourth Amendment protection does not extend to the information a person voluntarily reveals to a third party.[96] Accordingly, if historical CSLI is considered to be information that is voluntarily given to a third party, then it is presumed that the government obtainment of historical CSLI is not considered a search and no warrant is required.[97] To support this argument, many opponents of a warrant requirement standard cite to the Court's ruling in *United States v. Miller*.[98]

In *Miller*, the Supreme Court held that a person has no legitimate expectation of privacy to the voluntary information provided to a bank.[99] Before his trial, the respondent sought to suppress bank records obtained

---

91. *Id.*
92. Malone, *supra* note 26, at 723.
93. *See* United States v. Davis, 754 F.3d 1205, 1223 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th. Cir. 2014); *infra* Part IV.A–E.
94. *See infra* Part IV.A–E.
95. Malone, *supra* note 26, at 712, 733.
96. 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, 506 (2012).
97. *Id.*
98. 425 U.S. 435, 445–46 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
99. *Miller*, 425 U.S. at 444–45.

through a purportedly flawed subpoena.[100] The lower court denied his motion and respondent was subsequently convicted on conspiracy charges.[101] On appeal, the Fifth Circuit reversed, but the Supreme Court later affirmed the district court's denial of the motion to suppress.[102] Additionally, in its decision, the Supreme Court reasoned that when a person conveys personal information to a third party, that person anticipates that the third party will inevitably convey that personal information to the government.[103]

> The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress . . . the expressed purpose of which . . . to require records to be maintained because they [are useful] "in criminal . . . investigations and proceedings."[104]

Banks retain a record of their customers' accounts to comply with the Bank Secrecy Act, which is "merely an attempt to facilitate the use of a proper and longstanding law enforcement technique by insuring that records are available when they are needed."[105] The Court concluded that because customers are aware that the information within their account is kept by the bank—a third party—there is no Fourth Amendment right violated when that information is conveyed to law enforcement.[106]

In addition to citing *Miller*, challengers to the warrant requirement standard for historical CSLI also cite the Court's decision in *Smith v. Maryland*107 to bolster their argument.[108] In that case the Court held—three years after *Miller*—that a person does not have a reasonable expectation of privacy to the telephone numbers they dialed.[109] In *Smith*, the government obtained an installation of a pen register on the petitioner's phone to collect

100. *Id.* at 436.
101. *Id.* at 436–37.
102. *Id.* at 437, 440.
103. Rothstein, *supra* note 96, at 507 (citing *Miller*, 425 U.S. at 443).
104. *Miller*, 425 U.S. at 442–43 (quoting 12 U.S.C. § 1829b(a)(1) (1976)).
105. *Id.* at 444.
106. *Id.* at 444–45.
107. 442 U.S. 735 (1979).
108. *See id.* at 745–46 (1979); *Miller*, 425 U.S. at 446; *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010).
109. *Smith*, 442 U.S. at 745.

the phone numbers he dialed.[110] The police installed the pen register on the petitioner's phone without obtaining a warrant or court order.[111] The petitioner was suspected of participating in a robbery and subsequently making harassing phone calls to his victim.[112] With the help of the pen register, the police were able to identify the petitioner as the robbery suspect.[113] The victim was ultimately able to identify her robber, and thereafter, the petitioner was arrested.[114] Prior to his trial, the petitioner sought to suppress all evidence obtained from the pen register on the contention it violated his Fourth Amendment rights against unreasonable search and seizure.[115] The lower court ultimately denied the petitioner's motion to suppress and the appeal went all the way to the Supreme Court.[116] Eventually, the Supreme Court held that because the information is voluntarily conveyed to a third party, a person does not have a subjective expectation of privacy to the phone numbers he or she dials.[117] In addition, most people are aware that the carrier retains a record of the numbers dialed because they eventually appear on a monthly telephone bill.[118]

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[119]

The petitioner attempted to argue that he had a legitimate expectation of privacy because the telephone calls originated in his house.[120] Nevertheless, the Supreme Court quickly shut down this argument by stating "[r]egardless of his location, petitioner had to convey that number to the

110. *Id.* at 737.
111. *Id.*
112. *See id.*
113. *Id.*
114. *Smith*, 442 U.S. at 737.
115. *Id.* at 737–38.
116. *Id.*
117. *Id.* at 743–44; *see also* Fraser, *supra* note 57, at 588. "Further, in *Smith v. Maryland*, the Supreme Court found that the user of a telephone had voluntarily conveyed records of telephone numbers dialed when calls were made, and therefore assumed the risk that those records would be revealed to the police." Fraser, *supra* note 57, at 588.
118. *Smith*, 442 U.S. at 742.
119. *Id.* at 743.
120. *Id.*

telephone company in . . . the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference . . . ."[121] Even if he had an expectation of privacy to his dialed telephone numbers, the Supreme Court further noted that society is not willing to acknowledge this expectation of privacy as reasonable.[122]

B. *Historical CSLI: A Voluntary Disclosure to a Third Party*

The underlying policy argument in both *Miller* and *Smith* is identical: When a person voluntarily reveals information to a third party they surrender any legitimate expectation of privacy over that information.[123] Courts have extended the third party argument to comprise information regarding: "[C]redit card statements, electric utility records, motel registration records, and employment records."[124] Proponents of a warrant requirement, however, challenge this line of reasoning and contend "cell phones automatically register with cell phone towers and send location information without any voluntary action by the user."[125] Although this may be the case, the automatic registration of a cell phone with a tower is an acknowledged consequence of possessing a cell phone.[126]

> Moreover, cell phone subscribers who simply pay their monthly bills without looking at them and who do not have GPS functions on their phones are still likely to know that the government uses such techniques due to the high-profile crimes that law enforcement agencies have reported and solved with the help of CSLI.[127]

The Third Circuit, however, attempted to argue that a typical cell phone user likely does not even realize that a carrier retains their location

121. *Id.*
122. *Id.*
123. *Smith*, 442 U.S. at 743–44; *United States v. Miller*, 425 U.S. 435, 442–43 (1976); *see also* United States v. Graham, 846 F. Supp. 2d 384, 399 (D. Md. 2012). "Historical CSLI has been analogized with other types of personal records, such as bank records, that courts have ruled are [freely given] to a third party." Malone, *supra* note 26, at 739.
124. *Graham*, 846 F. Supp. 2d at 399.
125. Malone, *supra* note 26, at 739.
126. *Id.*
127. Fox, *supra* note 42, at 789.

information.[128] However, this argument can easily be invalidated.[129] When a cell phone user places a call, the user must undoubtedly anticipate that their carrier will determine their call location for billing purposes.[130] How would a carrier determine the proper billing rate for a cell phone call without determining the subscriber's location when making the call?[131] Therefore, a subscriber must recognize that their cell phone provider retains their location information as part of the ordinary course of business.[132]

An additional argument for why historical CSLI is considered a voluntary conveyance of information is because a cell phone user can easily turn off their phone, thereby preventing the registration of their location with a cell tower.[133] In addition, most cell phone thieves immediately turn off the stolen phone because they understand that their location will likely be traceable.[134] "[T]he prevalence of cell phones with GPS functions and subscribers' increased use of these services directly undermine the position that cell phone customers are not *voluntarily* sharing their location information with [cell site providers]."[135]

1. Comparison to *United States v. Davis*

Similar to the telephone numbers dialed in *Smith*,[136] and the bank information provided to the bank in *Miller*,[137] the defendant in *Davis*

---

128. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010); Malone, *supra* note 26, at 739.

129. *See* Malone, *supra* note 26, at 739.

130. *Id.* at 739–40.

131. *See id.*

> [A]s users become more aware of cell phone technology, there will no longer be a widespread lack of knowledge regarding the type of location data cell phone companies routinely collect. If people continue to use their cell phones even after they learn and understand how historical CSLI is gathered and maintained, they will have a much harder time arguing that the CSLI has not been voluntarily conveyed.

Id. at 740.

132. *Id.* at 739–40.

133. Malone, *supra* note 26, at 740.

134. Garth Johnston, *Smart Thieves Wise Up to Smart Phones: Turn 'Em Off to Disable Tracking*, GOTHAMIST (March 26, 2012, 12:01 PM), http://gothamist.com/2012/03/26/smart_crooks_wise_up_on_smart_phone.php.

135. Fox, *supra* note 42, at 788.

> Therefore, a cell phone user has no legitimate expectation of privacy in the CSLI that the [cell site provider] records when the user makes or receives a call because the subscriber has voluntarily shared this information with the [cell site provider] and assumes the risk that the [cell site provider] may turn the information over to law enforcement agencies.

Id. at 788–89.

136. Smith v. Maryland, 442 U.S. 735, 745 (1979).

voluntarily transmitted his location to cell towers in order to make and receive calls.[138] The carrier then retained the location information of the defendant for its personal business records.[139] "[H]istorical [CSLI] are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers. As part of the ordinary course of business, cell[] phone companies collect information that identifies the cell[] towers through which a person's calls are routed."[140]

C. *The Beeper Cases*

Soon after the decisions of *United States v. Knotts*[141] and *United States v. Karo*,[142] the Supreme Court decided two cases within a two-term period that addressed the issue of governmental use of tracking devices in determining the whereabouts of suspected drug manufacturers.[143] These two cases assist in determining whether a person has a reasonable expectation of privacy to his or her precise location.[144] Additionally, "[t]hese cases are especially apt when discussing historical CSLI because they dealt with a technology that many critics of the current interpretation of the SCA compare to cell phones: [T]racking devices."[145]

> Employing the use of beepers allows law enforcement agents to track the object the beeper has been attached to by following the emitted signals, similar to the way in which one can compute historic CSLI to create a general picture of the movements of a cell phone, but with greater accuracy and in real-time.[146]

In *Knotts*, law enforcement agents positioned a tracking beeper in a container that was holding chloroform that agents suspected was used by the defendants in their production of drugs.[147] Law enforcement agents were able to track the container to a remote cabin.[148] With the assistance of the

137. United States v. Miller, 425 U.S. 435, 444–45 (1976).
138. United States v. Davis, 754 F.3d 1205, 1209–10, 1216 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014).
139. *Id.* at 1209–10.
140. United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012).
141. 460 U.S. 276 (1983).
142. 468 U.S. 705 (1984).
143. Fox, *supra* note 42, at 780.
144. Malone, *supra* note 26, at 713.
145. *Id.*
146. Fox, *supra* note 42, at 780 (footnote omitted).
147. United States v. Knotts, 460 U.S. 276, 277 (1983).
148. *Id.*

beeper and surveillance of the defendant's cabin, the agents were able to obtain a search warrant.[149] During the execution of the search warrant, agents discovered a drug laboratory and subsequently arrested the defendant.[150] The defendant sought to suppress the evidence law enforcement obtained through the warrantless tracking of the beeper.[151] After his motion to suppress was denied, the defendant was convicted and sentenced for producing a controlled substance.[152]

On appeal, the Eighth Circuit reversed the defendant's conviction and found the use of the beeper to track the defendant was a violation of his Fourth Amendment rights.[153] The Supreme Court, however, reversed the Eighth Circuit's decision and found the defendant's expectation of privacy was not violated because the warrantless tracking of the beeper was not a search within the Fourth Amendment.[154] The Court reasoned that "[t]he governmental surveillance conducted by means of the beeper . . . amounted principally to the following of an automobile on public streets and highways."[155] Additionally, the Court noted that a person has no reasonable expectation of privacy when traveling in a car on a public road because that person voluntarily conveys that information to the public.[156] The Court therefore once again concluded that a person cannot have a reasonable expectation of privacy to what is voluntarily conveyed to the public.[157]

A similar fact pattern involving a beeper occurred in *Karo*.[158] After the defendants purchased cans of ether from a confidential informant that were used in the extraction of cocaine from clothes that had been imported into the United States, the government secured a warrant that allowed the installation and tracking of a beeper in one of the cans.[159] Once the defendant picked the cans of ether up from the informant, the agents then followed the defendant to his home.[160] After the cans were moved to a

149. *Id.* at 279.
150. *Id.*
151. *Id.*
152. *Knotts*, 460 U.S. at 279.
153. *Id.* at 279.
154. *Id*. at 285.
155. *Id.* at 281.
156. *Id.* at 281–82.

> When Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Knotts, 460 U.S. at 281–82.

157. *Id.* at 281–82.
158. United States v. Karo, 468 U.S. 705, 708 (1984).
159. *Id.*
160. *Id.*

number of locations, through the use of the beeper, the government agents finally discovered that the cans were at the house rented by the defendants.[161] The agents then obtained a warrant to search the house and subsequently discovered the defendants' cocaine and laboratory paraphernalia.[162] The defendants were consequently arrested and moved to suppress the evidence derived from the initial warrant to install the beeper.[163]

After the court of appeals affirmed the district court's decision to grant the defendant's suppression of evidence, the Supreme Court granted certiorari.[164] The Court ultimately decided that although the defendant's Fourth Amendment rights were not violated when the government installed the beeper on the ether can, the monitoring of the can when it was inside the defendant's home was considered an unreasonable search.[165] Unlike *Knotts*, as the Court noted, the beeper in *Karo* showed that it was inside the defendants' home.[166] The Court furthermore held that the use of a beeper to track a person in his or her private residence that is not open to visual surveillance is considered a search within the Fourth Amendment.[167]

Where exactly the beepers were broadcasting their precise location is the key difference between these two cases.[168] The most significant question to ask when one is studying electronic surveillance cases is "what kind of information can be collected and whether that sort of information would be freely available to, say, a passerby?"[169] Moreover, these two cases inevitably created a public/private distinction to evaluate the use of warrantless tracking devices and their potential Fourth Amendment implications.[170]

---

161. *Id.* at 708–10.

162. *Id.* at 710.

163. *Karo*, 468 U.S. at 710. "The [d]istrict [c]ourt granted respondents' pretrial motion to suppress the evidence seized from the . . . residence on the grounds that the initial warrant to install the beeper was invalid and that the . . . seizure was the tainted fruit of an unauthorized installation and monitoring of that beeper." *Id.*

164. *Id.* at 710–11.

165. *Id.* at 713, 715.

> The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.

Id. at 715.

166. *Karo*, 468 U.S. at 710, 715; United States v. Knotts, 460 U.S. 276, 284–85 (1983).

167. *Karo*, 468 U.S. at 714.

168. Malone, *supra* note 26, at 715.

169. *Id.* at 716.

170. Fox, *supra* note 42, at 782; *see also Karo*, 468 U.S. at 714; *Knotts*, 468 U.S. at 284.

1. CSLI Differs from Beeper Cases

Supporters of a warrant requirement for CSLI argue that the same analysis used in the beeper cases should be employed in CSLI cases.[171] Employing the same public/private analysis, however, would be superfluous.[172]

> [C]urrently CSLI is not consistently accurate enough to implicate the home of a suspect, but rather only indicates the general area where the call was made from, which may or may not give rise to the inference that the defendant was at home. *Knotts* and *Karo* make clear that acquiring location information about an object in the vicinity of the home or other private space, but not within its interior, is not a search.[173]

In addition, "historical CSLI does not convey information about the interior of a home."[174] Unlike the beeper cases that provide a precise location of the tracking device, historical CSLI typically only reveals the location of a cell phone within roughly 200 feet.[175]

> [T]he historical [CSLI] at issue identif[ies] only the closest cell[] tower to the Defendants' phones, and not the precise location of the Defendants themselves. . . . Indeed, even with an ever-denser cell[] tower grid, such precision is impossible. Moreover, even if cell site records could definitively indicate that an individual is in his home, that information only reveals that a person made or received a phone call while at home—in other words, non-incriminatory information that is clearly obtainable via the constitutional pen register at issue in *Smith v. Maryland*.[176]

---

171. Fox, *supra* note 42, at 789. "Further, as CSLI becomes increasingly accurate, it will cause historical CSLI to fall under the ambit of *Karo*, as that information will allow law enforcement to determine if a suspect is in his or her home." Fraser, *supra* note 57, at 609; *see also Karo*, 468 U.S. at 714.

172. *See* Fraser, *supra* note 57, at 611–12. "The tracker beeper cases simply do not carry over well to a tracking device that has other uses; there is a need for a different distinction in CSLI analysis." *Id.* at 612.

173. *Id.* at 609; *see also Karo*, 468 U.S. at 714; *Knotts*, 460 U.S. at 285.

174. Malone, *supra* note 26, at 737.

175. *Id.* "Unless a person is standing in the middle of a residence and the walls are 100 feet away in any direction, his historical CSLI will not be precise enough to prove that he is actually inside the walls of the residence and secluded from the public eye." *Id.*

176. United States v. Graham, 846 F. Supp. 2d 384, 404 (D. Md. 2012); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979); Malone, *supra* note 26, at 738. "CSLI cannot indicate *with certainty* anything about the interior of a private residence. Thus, the

Consequently, unlike the more precise tracking of a beeper, historical CSLI does not provide a precise location of a cell phone because the cell tower only gives an approximate location.[177] Because historical CSLI substantially differs from beeper tracking, "CSLI falls outside of the traditional Fourth Amendment protections. Accordingly, when a law enforcement agent uses voluntarily conveyed historical CSLI information to approximate a subscriber's location, it does not constitute a Fourth Amendment search."[178]

D. United States v. Jones

The most recent case that dealt with Fourth Amendment implications on tracking devices occurred in *United States v. Jones*.[179] In *Jones*, the government secured a search warrant to install a GPS on a vehicle that was registered to the respondent's wife.[180] The government suspected the respondent of trafficking drugs through his nightclub and accordingly sought the warrant to allow the government to install the electronic tracking device.[181] The warrant authorized the government to install and track the car in the District of Columbia for only ten days.[182] Disobeying the terms of the warrant, the government installed the device in Maryland on the eleventh day.[183] Signals from the device documented the vehicle's location within roughly one hundred feet.[184] With help from the tracking device, the government was able to obtain an indictment against the respondent and

---

Fourth Amendment does not protect historical CSLI, and current law does not require a warrant or probable cause to obtain historical CSLI." Malone, *supra* note 26, at 738.

177. Fox, *supra* note 42, at 789. "This information does not provide the actual location of the cell phone because CSLI only gives the cell tower location used to carry a call and because location calculations based on cell towers give only an approximation of a subscriber's phone's location." *Id.* at 789.

178. *Id.* at 790.

> If multiple cell sites record CSLI, the approximate location of the cell phone at the initiation of the call can be computed. This approximate location, however, provides the general area of the caller, not the exact location. A tracking beeper, on the other hand, can be traced to a precise location. . . . [H]istoric CSLI cannot show that a subscriber was at a particular place at a particular time; it can only show that the phone was in a general area.

Id. at 789–90.

179. United States v. Jones, No. 10-1259, slip op. at 1 (U.S. Jan. 23, 2012).

180. *Id.* at 1–2.

181. *Id.*

182. *Id.* at 2.

183. *Id.*

184. *Jones*, No. 10-1259, slip op. at 2.

several of his co-conspirators, charging them with conspiracy to distribute cocaine.[185]

Prior to trial, the respondent sought to suppress the evidence obtained from the GPS tracking, arguing that the installation and tracking of the GPS on the vehicle was an unreasonable search within the Fourth Amendment.[186] The court, however, only suppressed the evidence obtained through the GPS while the vehicle was parked in the garage of the respondent's house.187 Subsequently, the respondent was convicted at trial.[188] The District of Columbia Circuit reversed the conviction on the grounds that the evidence acquired from the warrantless tracking of the GPS violated the Fourth Amendment.[189]

On appeal to the Supreme Court, the majority opinion, written by Justice Scalia, indicated that the case was primarily about the physical intrusion by the government onto private property for the sole purpose of obtaining evidence.[190] "We have no doubt that such a physical intrusion would have been considered a *search* within the meaning of the Fourth Amendment when it was adopted."[191] The Court, therefore, predominantly based its decision on the common law trespass doctrine.[192] The physical trespass by the government to install the GPS device, outside the requirements set forth by the warrant, violated the respondent's Fourth Amendment right against unreasonable searches.[193]

1. Why *Jones* Analysis Does Not Apply

The Eleventh Circuit in *Davis* erroneously applied the analysis set forth by the Supreme Court in *Jones* to arrive at its holding.194 Several reasons exist why the analysis set forth in *Jones* cannot be applied to historical CSLI cases.[195]

185. *Id.* at 2–3.
186. *Id.* at 2.
187. *Id.*
188. *Id.* at 3.
189. *Jones*, No. 10-1259, slip op at 3.
190. *Id.* at 4.
191. *Id.* at 4.
192. *Id.* "The majority decided only that a search occurs when the government trespasses on an individual's property for the purpose of gathering information." Rothstein, *supra* note 96, at 501.
193. *Jones*, No. 10-1259, slip op. at 1–3, 12.
194. *See id.* at 3–4; United States v. Davis, 754 F.3d 1205, 1212, 1214 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014).
195. *Jones*, No. 10-1259, slip op. at 3–4; Fraser, *supra* note 57, at 620.

First, the Eleventh Circuit indicated that GPS tracking and CSLI are analogous.[196] As previously discussed, the tracking produced by a GPS and historical CSLI yield different levels of accuracy when determining an individual's location.[197] In *Jones*, the device was attached to a car, and the law enforcement agents tracked its movements in real-time.[198] In *Davis*, however, the government did not track the suspects movements in real-time; the government simply obtained historical CSLI which does not track an individual's precise real-time movements.[199] "Historical cell site location data is, as its name implies, historical—the information revealed by such data exposes to the government only where a suspect *was* and not where he *is*."[200]

In addition, unlike *Jones*, the agents in *Davis* obtained records from the defendant's cell phone carrier that only revealed the vicinity in which he made or received a cell phone call.[201] And, unlike *Jones*, "this information can only reveal the general vicinity in which a cell[] phone is used."[202] The court even noted that "[w]e do not doubt that there may be a difference in precision, but that is not to say that the difference in precision has constitutional significance."[203] This argument is flawed because a person does not have a legitimate expectation of privacy to everything, and a person's precise location is vital in determining whether their Fourth Amendment rights have been violated.[204] Therefore, the Eleventh Circuit erred when it compared the tracking device employed in *Jones* to the historical CSLI employed in *Davis*.[205]

Next, the analysis set forth in *Jones* cannot be applied to the *Davis* case because there was no trespass in *Davis*.[206] Nevertheless, although the court addresses this factual distinction, it still used *Jones* to arrive at its decision.[207]

> [I]n the controversy before us there was no GPS device, no placement, and no physical trespass. Therefore, although *Jones* clearly removes all doubt as to whether electronically transmitted

196. *Davis*, 754 F.3d at 1213.
197. *See supra* notes 172–78 and accompanying text.
198. *Jones*, No. 10-1259, slip op. at 2.
199. *Davis*, 754 F.3d at 1210–11; *see also* Fraser, *supra* note 57, at 613–14.
200. United States v. Graham, 846 F. Supp. 2d 384, 391 (D. Md. 2012).
201. *Jones*, No. 10-1259, slip op. at 2; *Davis*, 754 F.3d at 1210–11; *Graham*, 846 F. Supp. 2d at 392.
202. *Graham*, 846 F. Supp. 2d at 392; *see also Jones*, No. 10-1259, slip op. at 2.
203. *Davis*, 754 F.3d at 1216.
204. *See e.g.*, Fraser, *supra* note 57, at 609–13.
205. *See Davis*, 754 F.3d at 1213–14, 1216; Fraser, *supra* note 57, at 613.
206. *Davis*, 754 F.3d at 1214; *see also Jones*, No. 10-1259, slip op. at 4.
207. *Davis*, 754 F.3d at 1215; *see also Jones*, No. 10-1259, slip op. at 12.

> location information can be protected by the Fourth Amendment it is not determinative as to whether the information in this case is so protected. The answer to that question is tied up with the emergence of the privacy theory of Fourth Amendment jurisprudence. While *Jones* is not controlling, we reiterate that it is instructive.[208]

Such an emphasis on the Supreme Court's analysis set forth in *Jones* further demonstrates why the Eleventh Circuit got it wrong.[209] Because the obtainment of one's historical CSLI does not involve a physical trespass to one's property, the Eleventh Circuit should not have employed the trespass theory to analyze the possible Fourth Amendment implications.[210] Instead, the Eleventh Circuit should have employed the analysis set forth in *Katz*—to determine whether the defendant had a reasonable expectation of privacy that society was willing to accept as reasonable—to his CSLI.[211]

E. Katz *Analysis Applied to* Davis

If the Eleventh Circuit decided to instead employ the *Katz* analysis it would have found that the defendant had no reasonable expectation of privacy.[212] Conversely, even if the court found that the defendant had a reasonable expectation of privacy, it would have found that society would not be willing to accept that expectation of privacy as reasonable because his location was voluntarily conveyed to the public through his cell phone provider.[213]

The Eleventh Circuit stated that:

> [E]ven on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the

---

208. *Davis*, 754 F.3d at 1214; *see also Jones*, No. 10-1259, slip op. at 12.

209. *See Jones*, No. 10-1259, slip op. at 12; Fraser, *supra* note 57, at 620.

> While it remains to be seen what the lasting effect of *Jones* will be, the Court's narrow holding that the installation and use of the GPS device was a search provides little guidance on what the standard of proof should be to obtain historical CSLI records. First, with respect to cell phones, the government does not have to install the devise used to generate location information—the user is already carrying around his or her cell phone.

Fraser, *supra* note 57, at 620; *see also Jones*, No. 10-1259, slip op. at 12.

210. United States v. Graham, 846 F. Supp. 2d 384, 396 (D. Md. 2012).

211. Katz v. United States, 389 U.S. 347, 361 (1967); *see also Graham*, 846 F. Supp. 2d at 396.

212. *See Katz*, 389 U.S. at 361; *Graham*, 846 F. Supp. 2d at 396–401.

213. *See Graham*, 846 F. Supp. 2d at 398–99; Malone, *supra* note 26, at 733.

> exposure of the [CSLI] can convert what would otherwise be a private event into a public one. . . . [CSLI] is private in nature rather than being public.[214]

However, as previously indicated, "historical CSLI are the provider's business records, and are not protected by the Fourth Amendment."[215] Because the defendant's historical CSLI was retained by his cell phone provider within its ordinary course of business, the defendant had no expectation of privacy to those records and consequently his Fourth Amendment rights were not violated.[216] Therefore, because the Eleventh Circuit disregarded the third party doctrine in arriving at its decision, it got it wrong when it comes to historical CSLI and the Fourth Amendment.[217]

V. CONCLUSION

Requiring a warrant each time law enforcement wishes to obtain historical CSLI would hinder the efforts of law enforcement and slow down their ability to investigate crimes.[218] While society's dependence on cell phones continues to grow and the government's need to solve crimes continuously persists, a uniform standard to obtain historical CSLI needs to be addressed by Congress.[219] However, as the Third Circuit articulated, it is not for the courts to decide what standard should be employed to obtain these records, but it is for Congress to decide.[220] The Eleventh Circuit failed to follow its sister circuit in this regard.[221]

As discussed at length, historical CSLI is not protected by the Fourth Amendment.[222] The Stored Communications Act[223] helps protect citizens and enables law enforcement to efficiently do their job.[224] Because a cell phone user does not have a legitimate expectation to privacy to the records voluntarily conveyed to their cell phone provider, the Fourth Amendment is

---

214. United States v. Davis, 754 F.3d 1205, 1216 (11th Cir.), *reh'g granted en banc*, 573 F. App'x 925 (11th Cir. 2014).

215. *Graham*, 846 F. Supp. 2d at 398; *see also* U.S. CONST. amend IV.

216. *Graham*, 846 F. Supp. 2d at 398; *see also* U.S. CONST. amend IV.

217. *See* Davis, 754 F.3d at 1216–17; Graham, 846 F. Supp. 2d at 398–400.

218. Malone, *supra* note 26, at 744.

219. Fox, *supra* note 42, at 792.

220. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

221. *Davis*, 754 F.3d at 1216–17.

222. *See* Fox, *supra* note 42, at 792.

223. *See generally* Stored Communications Act § 201, 18 U.S.C. §§ 2701–2710 (2012).

224. Malone, *supra* note 26, at 745; *see also* 18 U.S.C. § 2703.

not implicated.[225] The Eleventh Circuit failed to analyze *Davis* properly and consequently its decision was misguided.[226]

After the submission of this Comment, the government filed a petition for rehearing en banc.[227] With a majority of judges agreeing in favor of rehearing, the Eleventh Circuit ultimately vacated the *Davis* decision.[228]

225. Malone, *supra* note 26, at 745.

226. *Davis*, 754 F.3d at 1210; *see also* United States v. Graham, 846 F. Supp. 2d 384, 403 (D. Md. 2012); Fraser, *supra* note 57, at 613; Malone, *supra* note 26, at 745.

227. *See* Davis, 754 F.3d at 1223.

228. *Id.*