Santa Clara Law Review

Volume 52 | Number 2 Article 5

1-1-2012

Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence

Scott A. Fraser

MAKING SENSE OF NEW TECHNOLOGIES AND OLD LAW: A NEW PROPOSAL FOR HISTORICAL CELL-SITE LOCATION JURISPRUDENCE

Scott A. Fraser*

TABLE OF CONTENTS

---

* J.D. Candidate 2012, Santa Clara University School of Law; B.A., History and Political Science, San Diego State University, 2006. I would like to thank Jason de Barros, Adriana Duffy-Hörling and Kyle Graham for their thoughtful comments and suggestions, and my Grandmother, Aloida Cisneros, for giving me strength and inspiration.

INTRODUCTION

Before the late 1980's an individual never left home without two essential items: their keys and wallet. Since that time, a third item has emerged: the cell phone. In June 2011, there were more than 320 million wireless subscribers in the United States, which constitutes one-hundred-and-two percent of the American population.[1] In fact, twenty-nine percent of all households in the United States are now wireless only.[2] Further, cellular service providers have

1. *Wireless Quick Facts: Mid-Year Figures*, CTIA-THE WIRELESS ASSOCIATION, http://www.ctia.org/media/industry_info/index.cfm/AID/10323 (last visited Dec. 30, 2011).

2. *Id.*

sought to make a cell phone user's keys and wallet obsolete by developing cell phones that double as both a car key and a method of payment, so that all the user requires in his daily life is his cell phone.[3]

Perhaps the most distinctive feature of the cell phone is that it is with us everywhere we go, making us available to both our colleagues and loved ones, as well as making them—and now the Internet—available to us.[4] In addition, location-based cell phone applications, such as Foursquare[5] and the "Places" feature on Facebook,[6] have capitalized on the fact that a cell phone is always with the user and the user's desire to share his location with others.[7] In order for a cell phone to properly function (i.e., make and receive calls or transmit data) it must be in constant connection with the cellular network.[8] As a cell phone communicates with the nearest cell towers, the cellular network records and stores this data, called cell-site location information (CSLI) in order for the network—and sometimes other users—to locate the cell phone.[9]

---

3. *See* Michael Fitzgerald, *Use Your Cell Phone Instead of Your Credit Card*, PC WORLD, (Sept. 19, 2005, 1:00 AM), http://www.pcworld.com/article/122590/use_your_cell_phone__instead_of_your_credit_card.html (reviewing various cell phone technologies that permit the user to link their credit card to his cell phone and thereby use his cell as a means of payment); Brian X. Chen, *Japanese Cell Phone Doubles as Car Key*, WIRED, (Sept. 24, 2008, 5:11 PM), http://www.wired.com/gadgetlab/2008/09/japanese-cell-p/ (reviewing a cell phone offering a car key function developed by Sharp and Nissan).

4. *See* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007).

5. *See* FOURSQUARE, http://foursquare.com/ (last visited Jan. 7, 2011) (allowing a user to "check in" at stores, restaurants, and other establishments, share this information with friends and earn a "badge" for the frequency with which the user visits those locations).

6. *See* FACEBOOK, http://www.facebook.com/places/ (last visited Jan. 7, 2011) (allowing the user to utilize the location-based feature to "share where they are," "connect with friends" and "find local deals").

7. *See* Kathryn Zickuhr & Aaron Smith, *4% of online Americans use location-based services*, PEW INTERNET (Nov. 4, 2010), http://www.pewinternet.org/Reports/2010/Location-based-services.aspx (stating that four percent of online Americans use location-based software services).

8. *See Electronic Communications Privacy Act Reform*: *Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 40 (2010) [hereinafter *May Hearings*] (statement of Prof. Orin Kerr).

9. *See id.*

Because a cell phone is always with the user, the CSLI records generated by a cellular network can provide a wealth of information about the individual user.[10] Understandably, law enforcement considers CSLI to be a very powerful investigative tool.[11] Magistrate Judge Stephen Wm. Smith, who testified before Congress in June 2010 and oversees applications for CSLI, estimates that the total number of electronic surveillance orders issued at the federal level exceeds 10,000 per year.[12] While early CSLI jurisprudence focused on *prospective* (real-time) CSLI,[13] recently the focus has shifted to *historical* CSLI[14] (the records of the

---

10. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 60 (2010) [hereinafter *June Hearings*] (statement of Richard Littlehale, Assistant Special Agent in Charge, F.B.I.).

11. *See id.*

12. *Electronic Communications Privacy Act Reform*: *Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 80 (2010) [hereinafter Smith, *May Hearings*] (statement of Hon. Stephen Wm. Smith). The exact number of electronic surveillance orders granted under the ECPA is unknown. *Id.* The Attorney General is required to report to Congress the number of pen registers requested. 18 U.S.C. § 3126 (2011). There is no sister reporting requirement for information obtained under § 2703. 18 U.S.C. § 2703(d) (2011).

13. *In re* Application of the United States of America for an Order Authorizing the Installation and Use of the Pen Register Device, a Trap and Trace Device, and for Geographic Location Information, 497 F. Supp. 2d 301 (D.P.R. 2007); *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the release of Subscriber and Other Information; and (3) authorizing the disclosure of Location-Based Services, *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Location of Cell Site Origination and/or Termination, Case Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006); *In re* Application of The United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678 (W.D. La. 2006); *In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *see also* Kevin McLaughlin, Note, *Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L.J. 421 (2007) (reviewing *prospective* CSLI jurisprudence).

14. United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL

communication between the cell phone and the cellular network generated and retained by a cellular service provider).[15] When discussing historical CSLI, many early cases and law review articles agreed that the information was obtainable under a lesser standard of proof than prospective CSLI.[16]

Recently, the Third Circuit became the first United States Court of Appeals to decide what the appropriate standard of proof was for law enforcement to obtain historical CSLI under the Stored Communications Act (SCA) and the Fourth Amendment, but the mixed result of the case does not answer the question convincingly.[17] Frustrated by Fourth

---

4200156 (N.D. Ga Apr. 21, 2008); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info., 622 F. Supp. 2d 411 (S.D. Tex. 2007); *In re* Applications of the United States of America for an Order Authorizing Continued use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Auth. on Tel. No. (XXX) XXX-XXXX and any Subsequently Assigned Tel. No., 530 F. Supp. 2d 367 (D. Mass. 2007); *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007); *see also* Patrick T. Chamberlin, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009) (reviewing *historical* CSLI jurisprudence).

15. *See May Hearings*, *supra* note 8, at 34 (statement of Prof. Orin Kerr).

16. *See Suarez-Blanca*, 2008 WL 4200156 (denying defendant's motion to suppress historical CSLI evidence that had been ordered disclosed by a magistrate judge under the Stored Communications Act standard); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info., 622 F. Supp. 2d 411 (S.D. Tex. 2007) (granting government access to both prospective and historical CSLI); *In re* Applications of the United States of America for an Order Authorizing Continued use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Auth. on Tel. No. (XXX) XXX-XXXX and any Subsequently Assigned Tel. No., 530 F. Supp. 2d 367 (D. Mass. 2007) (denying government access to prospective CSLI and granting government access to historical CSLI); *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007) (granting government access to historical CSLI); *see also* Adam Koppel, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1068–69 (2010) (stating that historical CSLI is limited in value and produces a lower level of concern from privacy advocates).

17. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 316 (3d Cir. 2010) (concluding that the SCA provides a "sliding

Amendment precedent and the current statutory framework, the Third Circuit concluded: "The considerations for and against such a requirement [a lesser standard of proof for historical CSLI] would be for Congress to balance. A court is not the appropriate forum for such balancing, and we decline to take a step as to which Congress is silent."[18]

Congress answered that call. In May, June, and September of 2010, Congress held fact-finding hearings to determine what changes needed to be made to the existing statutory framework.[19] The goals of Congress in creating new legislation on this topic were to balance an individual's right to privacy with the government's need to obtain evidence to prevent and investigate crime and respond to emergency circumstances.[20] In May 2011, Senator Leahy of the Senate Judiciary Committee introduced a bill in the U.S. Senate to amend the Electronic Communications Privacy Act (of which the SCA is a smaller part).[21] The legislation has been sent to the Senate Judiciary Committee and is currently being considered in the 112th Congress, First Session.[22] The potential impact of the proposed legislation will be discussed in Part III.A.

In addition, just before publication of this Comment the Supreme Court issued its decision in the GPS tracking case *United States v. Jones* (formerly known as *United States v. Maynard*). The Court's decision in that case and the implications of the decision for historical CSLI jurisprudence

---

scale" by which a judge can, at his or her discretion, grant an order for historical CSLI or require a warrant).

18. *Id.* at 319.

19. *See May Hearings*, *supra* note 8 (statement of Prof. Orin Kerr); *June Hearings*, *supra* note 10; *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Sen. Comm. on Judiciary*, 111th Cong. (2010) [hereinafter *September Hearings*].

20. *September Hearings*, *supra* note 19, Prepared Statement at 1 (Statement of James X. Dempsey, Esq., V.P., Center for Democracy and Technology) *available at* http://judiciary.senate.gov/pdf/10-09-22Dempsey Testimony.pdf. Another goal of Congress is to instill consumer confidence in communications technology. *Id.*

21. Rachelle Dragani, *US Senate Sinks its Teeth into Online Privacy Reform*, TECHNEWSWORLD (May 18, 2011, 11:40 AM), http://www.technewsworld.com/story/72477.html.

22. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

will be discussed in Part III.B.

The subject of this Comment is historical CSLI generated through cell phone calls.[23] Using the current statutory framework, Fourth Amendment precedent, and previous CSLI case law, this Comment suggests a new legal framework for the standard of proof required to obtain historical CSLI. This approach focuses on the user's active versus idle use of a cell phone. When a phone is in active use—such as when making or receiving a call—the information should be obtainable under a "specific and articulable facts standard," which is a lesser standard of proof than for a warrant.[24] However, when the phone is idle, the data generated by the cellular network should only be accessible under a probable cause standard.[25] An active use distinction will help to simplify how the current statutory framework is applied to historical CSLI and provide a workable solution that comfortably meshes with the existing statutes. In addition, this proposal will unify Fourth Amendment precedents that at times conflict.

First, Section I will discuss how the technology of CSLI works, what kind of data is stored by cellular service providers, what changes can be expected from advancements in future technology, and how law enforcement uses the data.[26] Next, the Comment will discuss the current statutory framework, Fourth Amendment precedent, and existing historical CSLI jurisprudence.[27] Section II will identify the legal problem to be discussed[28] and will analyze historical CSLI under the existing statutory framework and Fourth Amendment jurisprudence.[29] Section III will discuss the proposed solution to the current legal problem[30] followed by the conclusion.[31]

---

23. Text messages are outside the scope of this Comment: law enforcement requests for historical CSLI often do not request text message information. *See supra* notes 13, 14, 16.

24. *See infra* pp. 11–12.

25. *See infra* pp. 11–12.

26. *See infra* Part I.A–B.

27. *See infra* Part I.C–E.

28. *See infra* Part II.A.

29. *See infra* Part II.A.4–B.

30. *See infra* Part III.

31. *See infra* Conclusion.

I. BACKGROUND INFORMATION: WHAT IS HISTORICAL CELL-SITE LOCATION INFORMATION?

A. How Cell Phones Connect to the Cellular Network

In order for the cellular network to connect incoming calls to a user's cell phone and for the user to make outgoing calls, the cell phone must constantly relay its location to the nearest cell tower[32] and other towers close by.[33] Each phone has a Mobile Identification Number (MIN)—a ten-digit number that another user dials to call the phone; and an Electronic Serial Number (ESN)—a unique, unchangeable number assigned by the manufacturer.[34] Through a process called "registration," which occurs approximately every seven seconds, a cell phone identifies itself to the cellular network by relaying its MIN and ESN to the nearest tower and other towers nearby.[35] The phone registers with the cell tower that has the strongest radio signal, as well as up to six other cell towers nearby.[36] The cell phone then sorts and ranks these towers according to which signal is the strongest and the weakest.[37] This process occurs continuously and automatically as long as the phone is turned on.[38] The signals sent during registration are transmitted on a separate frequency, distinct from those that transmit voice and data to

32. The basic composition of a cell phone network is a series of grids and networks. The cell tower (base station) is the smallest part of each grid, which is controlled by a base station controller. Each base station controller reports to a larger network called a Location Area Code (LAC). Each LAC could contain anywhere from 100 to 125 cell towers, and is controlled by a mobile switching center (MTSO), where all types of data are recorded. Transcript of Record at 7–8, United States v. Sims, No. 06-674 (E.D. Pa. Nov. 13, 2007) (testimony of William Shute), *available at* http://www.eff.org/files/filenode/celltracking/shutetestimony.pdf [hereinafter Shute Testimony].

33. *See* McLaughlin, *supra* note 13, at 426.

34. *See* Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 309 [hereinafter *Who Knows Where You've Been*].

35. McLaughlin, *supra* note 13, at 426; *June Hearings*, *supra* note 10, at 13 (statement of Prof. Matt Blaze).

36. *See* McLaughlin, *supra* note 13, at 426; *June Hearings*, *supra* note 10, at 13 (statement of Prof. Matt Blaze).

37. *June Hearings*, *supra* note 10, at 13 (statement of Prof. Matt Blaze); Shute Testimony, *supra* note 32, at 11.

38. McLaughlin, *supra* note 13, at 426.

the phone.[39] As the user and the phone move through the cellular network, the cell phone continually sorts and ranks the nearest cell towers as the connection to one tower grows weaker and the connection to another tower grows stronger. This information is used by the cellular-telephone service provider (CSP) to locate the phone within the cellular network whenever the cell phone receives a call.[40] When the user is called, the CSP sends a signal through the entire cellular network, which locates the phone based on where it last registered.[41] A similar process works in reverse when the user makes a call.[42]

1. The Level of Information Retained and Stored by Cellular Service Providers

Historical CSLI is "non-content" information: information that the cellular network generates and uses in order to deliver the call, as opposed to the content of the conversation.[43] Every cellular-telephone service provider (CSP) stores this information, but the amount of information stored by each CSP depends on the technology,[44] and the business decisions that each company makes regarding data retention.[45] Historical CSLI stored by wireless providers can

39. *Id.*

40. McLaughlin, *supra* note 13, at 426; Shute Testimony, *supra* note 32, at 8; *June Hearings*, *supra* note 10, at 13 (statement of Prof. Matt Blaze). The cell towers measure the strength of the signal using either one or both of the two methods to measure the signal strength, Time Difference of Arrival (TDOA) or Angle of Arrival (AOA). TDOA measures the amount of time that it takes for the signal from a tower to travel to a user's phone, and from this measurement it is possible to estimate the distance between the tower and phone because radio waves move at a constant rate. AOA measures the angle at which the phone's signal arrives at the tower and uses that information to calculate the approximate location of the phone. Based on these measurements, the MTSO will then direct the phone to switch to the nearest tower with the strongest signal. *See Who Knows Where You've Been*, *supra* note 34, at 308–09.

41. *See* Shute Testimony, *supra* note 32, at 8.

42. McLaughlin, *supra* note 13, at 426.

43. *See May Hearings*, *supra* note 8, at 34 (statement of Prof. Orin Kerr).

44. Most, if not all cellular telephone service providers (CSPs) use one of three different technologies, which all operate in essentially the same fashion. T-Mobile and AT&T use Global Standard Mobile Communications (GSM), Verizon and Sprint use Code Division Multiple Access (CDMA), and Nextel uses Integrated Digital Enhanced Network (IDEN). Shute Testimony, *supra* note 32, at 4–5.

45. *Id.*

be separated into two categories: limited CSLI, which is the data created during the beginning and end of a call, and unlimited CSLI, which is all of the signaling information collected during the call and when the phone is idle.[46]

While most, if not all, wireless providers record and store limited CSLI,[47] others may also store unlimited CSLI[48]—including regularly updated, accurate location information.[49] As an example of what kind of information is stored, in 2009 Nextel stored the date, time, and duration of the calls as well as the cell tower when the call is made, the cell tower in the event of a change, and the cell tower when the call is terminated.[50] Historical CSLI is stored for long periods of time because it is extremely useful to CSP.[51] This information is used by CSPs for business, marketing and technical purposes.[52]

2. Current Cell Tower Configurations and Continued Growth

Cell towers can only handle a certain number of calls at a given time depending on the amount of radio spectrum bandwidth allocated to the CSP.[53] As a result, in more

46. *June Hearings*, *supra* note 10, at 99 (statement of Hon. Stephen Wm. Smith).

47. *See* Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 549 (2007).

48. *See* ELECTRONIC SURVEILLANCE MANUAL, UNITED STATES DEPARTMENT OF JUSTICE 42 (2010), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

49. *See June Hearings*, *supra* note 10, at 27 (statement of Prof. Matt Blaze).

50. Shute Testimony, *supra* note 32, at 10, 12–13. Additionally, how long the data is stored depends on the service provider and the technology. In general, given the low cost of storing data and the invaluable use of the data (discussed below), many service providers store the data as long as possible. Some providers divide their records into two classes: "billing records," which comprise the records of incoming and outgoing calls and the tower location that served them, and "maintenance records," which may include far more detailed information, such as records of when subscribers' handsets move through the network even when no calls are being made. *See also May Hearings*, *supra* note 8, at 34 (statement of Prof. Orin Kerr); *June Hearings*, *supra* note 10, at 16, 135 (statement of Prof. Matt Blaze).

51. *See June Hearings*, *supra* note 10, at 16 (statement of Prof. Matt Blaze).

52. Shute Testimony, *supra* note 32, at 10. Technically, the information tells CSP's where old infrastructure is redundant and where new infrastructure is needed. Marketing and business wise, the information is used to see how customers are using their phones. *See June Hearings*, *supra* note 10, at 16, 95.

53. *See June Hearings*, *supra* note 10, at 15, 26.

densely populated areas, the cell towers must be closer together in order to accommodate the increased number of users in that area.[54] New cellular data services such as 3G and 4G internet create similar pressure on the available spectrum bandwidth, usually requiring more densely populated cell towers.[55] In rural areas, there may be cell towers in a configuration covering several miles in diameter; but the trend in urban areas has been to install cell towers in increasingly smaller service areas called microcells, picocells and femtocells, which serve very specific locations, such as a floor of a building or even an individual room, such as a waiting room.[56]

B. Law Enforcement Uses of Cell-Site Location Information: What Does it all Mean?

First, it is important to understand what kind of information is sought by law enforcement from CSPs through the SCA. Law enforcement requests for CSLI vary greatly. Sometimes historical CSLI requests are only for limited CSLI[57] and other times are for unlimited CSLI as well;[58] other orders can be unclear as to what kind of information is being

54. *Id.*
55. *Id.* at 26.
56. *Id.* at 15–16.
57. *See, e.g.*, *In re* Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 679 (W.D. La. 2006) (requesting "the location of the cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and, if reasonably available, during the progress of a call for the subject telephone number.").
58. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) ("Each application identically defined the requested information as 'the antenna tower and sector to which the cell phone sends its signal, specifically including the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state.' In other words, the Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info., 622 F. Supp. 2d 411, 412 n.1 (S.D. Tex. 2007) (stating in the request that "call detail records also include a record of incoming calls and the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state.").

requested.[59] The time period over which CSLI records are requested can also vary dramatically.[60]

CSLI is most useful to law enforcement to show with whom a suspect communicates, from where, at what time, and for how long.[61] Law enforcement analyzes historical CSLI by looking at what cell tower the phone is communicating with, and what the signal strength of that call was.[62] If the phone communicates with a single tower during the entire duration of the call, the phone is in very close proximity to the tower.[63] If the phone shifts between two different cell towers during the course of a call, the phone is in the middle of an overlapping area of coverage between the two different cell towers.[64] The advantages of using CSLI as opposed to other location-based technologies is that many, if not all, adults already have a cell phone and law enforcement is therefore spared the trouble of having to install the device on the suspect's car or person.[65] CSLI is useful in instances where law enforcement does not yet have probable cause (the standard of proof required for a warrant).[66] This information is often used as a "stepping stone" for officers to request authorization from courts for more intrusive types of surveillance and searches, such as a wiretap authorized by a warrant.[67]

---

59. *See, e.g.*, *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571 (W.D. Tex. 2010) (failing to adequately state what kind of CSLI is being requested).

60. *See In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 11-MC-0113, 2011 WL 679925 (E.D.N.Y. Feb. 16, 2011) (requesting a 3 day period, a 6 day period, and a 12 day period); *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897, 2010 WL 5437209, at *1 n.3 (E.D.N.Y. Dec. 23, 2010) (requesting 113 days).

61. *September Hearings*, *supra* note 19, at 59 (statement of James A. Baker, Associate Deputy Att'y Gen.).

62. *See* Shute Testimony, *supra* note 32, at 19–20.

63. *See id.* at 22.

64. *See id.* at 8.

65. *See* Clark, *supra* note 4, at 1413.

66. *See id.* at 1414.

67. *June Hearings*, *supra* note 10, at 57 (statement of Richard Littlehale, Assistant SAC, F.B.I.); *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age*, 112th Cong. 4

C. Stored Communications Act: Law Enforcement Access to Historical Cell-Site Location Information

To acquire historical CSLI law enforcement must obtain a court order requiring a CSP to disclose the information.[68] Title II of the Electronic Communications Privacy Act (ECPA), known as the Stored Communications Act, regulates government access to wire and electronic communications.[69] The standard of proof required under the SCA for law enforcement to obtain historical CSLI, as well as the precise application of the statute to historical CSLI remains uncertain. First, an overview of the statutory scheme is essential.

The primary statute that governs the disclosure of CSLI is 18 U.S.C. § 2703.[70] Section 2703(c)(1) provides in pertinent part:

> (c) Records concerning *electronic communication service* or remote computing service. (1) 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* (*not including the contents of communications*) . . . .[71]

In order for historical CSLI to be available under 18 U.S.C. § 2703(c)(1), three qualifications must be met: first, 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.[72]

First, the CSP must be a provider of an "electronic communication service." Under the SCA, in order to qualify

---

(2011) [hereinafter *April Hearings*] (statement of James A. Baker, Associate Deputy Att'y Gen.).

68. McLaughlin, *supra* note 13, at 428.

69. *See June Hearings*, *supra* note 10, at 2 (statement of F. James Sensenbrenner, Rep. WI).

70. *See* 18 U.S.C. § 2703 (2011).

71. 18 U.S.C. § 2703(c) 2011 (emphasis added).

72. *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 79–80 (D. Mass. 2007). Content information is governed by sections 2703(a)–(b). *See* 18 U.S.C. § 2703(a)–(b) (2011).

as an electronic communications service provider the CSP must provide users with the ability to "send or receive wire or electronic communications."[73] A wire communication is:

> [A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities . . . .[74]

The Act defines an electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[75] There is little debate that historical CSLI qualifies as one or both of these definitions,[76] but which definition CSLI is categorized as has been the subject of litigation.[77] Second the data may not be content information under the meaning of the SCA. The SCA defines content as "any information concerning the substance, purport, or meaning of that communication."[78] Historical CSLI falls outside of the definition of content, and instead is classified as a "record or other information pertaining to a subscriber . . . or customer."[79]

Third, the data must be a "record or other information pertaining to a subscriber to or customer of," an electronic communications service.[80] Neither the term "record" nor "information" is defined by the SCA, but in the relevant context courts have found record to mean something stored or

---

73. 18 U.S.C. § 2510(15) (2011).

74. 18 U.S.C. § 2510(1).

75. 18 U.S.C. § 2510(12).

76. *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 79–80 (D. Mass. 2007).

77. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 309–10 (3d Cir. 2010); Chamberlin, *supra* note 14, at 1775–76.

78. 18 U.S.C. § 2510(8) (2011).

79. 18 U.S.C. § 2703(c)(1) (2011).

80. *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

archived, and information to mean data.[81] Finding that stored CSLI data recorded from a cell tower is a record and that CSLI data is information, courts have found that CSLI is a "record or other information."[82] While most courts agree that historical CSLI is obtainable under the SCA, there is disagreement over the standard of proof required.

1. Standard of Proof: What Level of Proof Must Law Enforcement Show?

Historical CSLI is available under § 2703(c)(1) only when law enforcement: (A) obtains a warrant, or (B) obtains a court order under § 2703(d) (a "section (d) order").[83] The § 2703(d) standard of proof required for a court order under § 2703(c)(1)(B) is:

> (d) Requirements for court order. A court order for disclosure . . . shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that . . . *the records or other information sought*, are relevant and material to an ongoing criminal investigation.[84]

This standard is an intermediate standard, less than that of a probable cause, but more than required for a pen register or trap-and-trace device.[85]

While the standard of proof for both wire communication and electronic communication is the same, there is good reason for the government and the courts to be careful about how the information sought is classified.[86] Under the SCA, any communication from a "tracking device" is excluded from the definition of "electronic communication."[87] Section 3117 defines a tracking device as: "an electronic or mechanical device which permits the tracking of the movement of a

81. *Id.*
82. *Id.*
83. 18 U.S.C. § 2703(c) (2011).
84. 18 U.S.C. § 2703(d) (2011) (emphasis added).
85. *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010). A pen register is a device or process which records the telephone numbers of outgoing calls. A trap-and-trace device captures the telephone numbers of incoming calls. *See* 18 U.S.C. § 3127(3)–(4) (2011).
86. *See* notes 87–89 and accompanying test (discussing 18 U.S.C. § 3117 exception to the definition of electronic communication).
87. 18 U.S.C. § 2510(12)(c) (2011).

person or object."[88] Therefore, if the "electronic communication" sought under § 2703(c)(1) is information derived from a device which "permits the tracking of movement of a person or object" that electronic communication cannot be obtained under § 2703(c)(1).[89]

2. Legislative History: The Scope of the Stored Communications Act

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) which updated 18 U.S.C. § 2703 to its current state.[90] During Senate and House hearings for CALEA, then-Director of the FBI Louis Freeh testified regarding the purpose of the bill.[91] Director Freeh stated that "[l]aw enforcement's requirements set forth in proposed legislation include an ability to acquire 'call setup information.' This information relates to dialing type information—information generated by a caller which identifies the origin, duration, and destination of a wire communication, the telephone number or similar communication address."[92] When asked whether or not this information could be used to locate an individual, Director Freeh stated:

> Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view.[93]

The legislative intent of CALEA and the meaning of Director Freeh's testimony has been the subject of debate for courts.[94]

---

88. 18 U.S.C. § 3117 (2011).

89. 18 U.S.C. § 2510(12)(c) (2011).

90. *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010).

91. Louis J. Freeh, Director, F.B.I., *Police Access to Advanced Communication Systems*: *S. J. Judiciary on Tech., Law, Civil and Constitutional Rights* (Mar. 18, 1994), *reprinted in* Federal Document Clearing House, 1994 WL 223962 *33.

92. *Id.*

93. *Id.*

94. *See In re* Application of the United States of America for an Order

Some courts have interpreted Director Freeh's testimony to mean that a warrant is required to obtain historical CSLI, while other courts have interpreted the testimony to say that a section (d) order is sufficient.

D. Current Fourth Amendment Jurisprudence

The Fourth Amendment to the Constitution provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[95] In order to determine whether a search has taken place for the purposes of the Fourth Amendment, the Supreme Court held in *United States v. Katz* that there is a twofold analysis: first, did the person have an actual (subjective) expectation of privacy, and second, was that expectation one that society is prepared to recognize as objectively reasonable.[96] The Supreme Court further elaborated that the home is a place where individuals have a subjective expectation of privacy that is objectively reasonable in the view of society.[97] Because there is no Supreme Court authority directly on point, courts have analogized historical CSLI to other lines of cases. One area of case law focuses on the disclosure of information to third parties, another area focuses on electronic surveillance through the use of "beepers," and other courts have found the prolonged surveillance doctrine announced in *United States v. Maynard* persuasive.

1. Assumption of the Risk: Third Party Disclosure

Under the Fourth Amendment a "person has no legitimate expectation of privacy in information he

---

Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 763 (S.D. Tex. 2005).

95. U.S. CONST. amend. IV.

96. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In *Katz*, government agents intercepted the contents of a telephone conversation by attaching an electronic listening device to a public telephone booth. The Court found that Katz had a reasonable expectation of privacy while using the telephone booth and that the government's activity of listening to and recording his words was a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353; *see also* Smith v. Maryland, 442 U.S. 735, 739 (1979).

97. *Katz*, 389 U.S. at 351.

voluntarily turns over to third parties."[98] The Supreme Court has found that where a person has voluntarily conveyed certain information to a third party, he or she has assumed the risk that the third party could disclose the information to law enforcement.[99] For example, in *United States v. Miller* the Supreme Court found that the customer of a bank did not have a reasonable expectation of privacy in the financial documents that he voluntarily conveyed to the bank.[100] The Court found that the customer assumed the risk that those records could be accessible by the government, even if that information was revealed to the bank on the assumption that it will only be used for a limited purpose and in confidence.[101]

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.[102] First, the Court distinguished *Katz*, stating that pen registers did not acquire the contents of communications.[103] Second, the Court held that the telephone user had no subjective expectation of privacy because "[a]ll 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."[104] In addition, the user of the phone did not have an objective expectation of privacy because this expectation was not "one that society [was] prepared to recognize as 'reasonable.'"[105] Whether the assumption of the risk doctrine applies to historical CSLI has been a subject of litigation in courts.

2. Use of Electronic Surveillance to Track a Suspect: The Beeper Cases

Other courts have sought guidance from the beeper cases to determine if a cell phone user has a reasonable expectation

98. *Smith*, 442 U.S. at 743–44.
99. *Id.* at 735, United States v. Miller, 425 U.S. 435, 443 (1976).
100. *Miller*, 425 U.S. at 443.
101. *Id.*
102. *Smith*, 442 U.S. at 744.
103. *See id.* at 741.
104. *Id.* at 742.
105. *Id.* at 743–44 (internal citations omitted).

of privacy in his CSLI records. The beeper cases concerned the use of tracking devices for surveillance purposes and whether they infringed upon a reasonable expectation of privacy and therefore constituted a search within the meaning of the Fourth Amendment.[106] In *United States v. Knotts*, the police used a radio transmitter, called a "beeper," to track the movement of the suspect on public roadways.[107] The Court held that the defendant's Fourth Amendment rights were not violated.[108] The government surveillance conducted through the use of the beeper amounted to no more than following the defendant's car on public streets and highways - an area where a person did not have a reasonable expectation of privacy.[109] The Court further added that the Fourth Amendment did not prohibit police from augmenting what they could normally have observed (the car on public streets) with the use of technology (the beeper).[110]

Shortly thereafter, the Supreme Court imposed an important limitation on its holding in *Knotts*.[111] In *United States v. Karo*, the government used a beeper in a similar fashion to *Knotts* by installing the device in a can of ether.[112] There, the Court found that the defendant's Fourth Amendment rights had been violated because agents used the beeper to determine that the chemicals were inside the interior of the suspect's home, an area where the suspect had a reasonable expectation of privacy.[113] The Supreme Court found that the use of technology to gather information about the interior of the home distinguished the case from *Knotts*, as the information gathered in *Karo* could not have been visually verified.[114] The beeper cases have led courts to consider two questions with respect to CSLI: is historical CSLI sufficiently analogous to a beeper for *Knotts* and *Karo* to control, and does historical CSLI invade the privacy of the

106. *See* United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).
107. *Knotts*, 460 U.S. at 281.
108. *Id.* at 281.
109. *Id.*
110. *See id.* at 282.
111. *See infra* Part I.D.3.
112. *Karo*, 468 U.S. at 708–09.
113. *Id.* at 714.
114. *Id.* at 715.

home?

3. The Prolonged Surveillance Doctrine: Does the Duration of the Surveillance Matter?

Recently, the D.C. Circuit issued an opinion that has been very influential in historical CSLI cases. In *United States v. Maynard*, the police fixed a GPS tracking device to the defendant's automobile without a warrant.[115] In *Maynard*, the court did not concentrate on the location of the surveillance (roadways or the home), but instead focused on the *duration* of the surveillance.[116] The D.C. Circuit concluded that *Knotts* was not controlling under the facts of the case, reasoning that in *Knotts* the Supreme Court distinguished between limited information obtained from a beeper (movements during a discrete journey), and more sustained and continuous monitoring, such as with the defendant in *Maynard*.[117] The court found that the defendant had a reasonable expectation of privacy under *Katz*,[118] reasoning that his continuous movements—twenty-four hours a day over the course of twenty-eight days—were not exposed to the public.[119] The court further held that the whole of one's movements over the course of a month were not exposed to the public, because there was zero likelihood that anyone, including police, would observe all of those movements.[120] The court then reasoned that the entirety of defendant's movements revealed more than each individual movement, and that the whole was therefore greater than the sum of its parts—the entire picture of defendant's actions over the course of a month.[121]

However, it is important to note that all courts have not accepted this doctrine. In *United States v. Pineda-Moreno*, the Ninth Circuit declined to find the use of a GPS tracking device, used in a similar fashion to *Maynard*, was an

115. United States v. Maynard, 615 F.3d 544 (2010), *reh'g en banc denied sub nom.*; United States v. Jones, 625 F.3d 766 (2010), *cert. granted* 131 S. Ct. 3064.
116. *Id.*
117. *Id.* at 555–56.
118. *Id.* at 563–64.
119. *Id.* at 558.
120. *Id.*
121. *Id.* at 544.

impermissible search.[122] "The only information the agents obtained from the tracking devices was a log of the locations where Pineda-Moreno's car traveled, information the agents could have obtained by following the car."[123]

Using the assumption of the risk doctrine, the beeper cases, and the prolonged surveillance doctrine, courts have attempted to analyze whether law enforcement use of historical CSLI is a search within the meaning of the Fourth Amendment and therefore requires a warrant based on probable cause.

E. Historical CSLI Case Law: The Search for a Statutory and Fourth Amendment Solution

1. Early CSLI Jurisprudence

In many historical CSLI applications, the court undertakes a two step analysis: (1) is historical CSLI obtainable under the SCA; and if so, (2) does the acquisition of historical CSLI require a warrant under the Fourth Amendment. In the early discussion of CSLI, many cases and law review articles agreed that historical CSLI, as a "record or other information," was obtainable under a § 2703(d) showing of "specific and articulable facts."[124] In some cases, historical CSLI was allowed under the statutory and Fourth Amendment framework even though prospective CSLI was denied.[125]

Early historical CSLI cases largely found that the user of a cell phone did not have a reasonable expectation of privacy

---

122. United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010), *reh'g en banc denied,* 617 F.3d 1120 (9th Cir. 2010).

123. *Id.* This decision was the subject of a scathing dissent by Chief Judge Kozinksi in which he evoked images of *1984*'s Oceania. *Pineda-Moreno*, 617 F.3d at 1126 (Kozinski, C.J., dissenting).

124. *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007); HON. JAMES CARR & PATRICIA L. BELLIA, 1 LAW OF ELECTRONIC SURVEILLANCE § 4:84, ACQUISITION OF CELL SITE LOCATION DATA (Sept. 2011) (listing all of the early pro (d) order CSLI decisions). *See also supra* note 14 and accompanying cases.

125. *See In re* Applications of the United States of America for an Order Authorizing Continued use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Auth. on Tel. No. (XXX) XXX-XXXX and any Subsequently Assigned Tel. No., 530 F. Supp. 2d 367, 368 (D. Mass. 2007).

under the "assumption of the risk" framework.[126] A typical example is *United States v. Suarez-Blanca*, where the Court found that although a cell phone user might have a subjective expectation of privacy with respect to CSLI,[127] this expectation of privacy was not objectively reasonable under the assumption of the risk doctrine.[128] Further, these early CSLI cases did not find that the accuracy of surveillance conducted was sufficient to implicate the Fourth Amendment under *Karo* because CSLI did not indicate the location of defendants in the home or other private locations.[129]

2. Current CSLI: Statutory and Fourth Amendment Challenges

Historical CSLI began to receive greater attention in 2008 when Magistrate Judge Lenihan authored the opinion that was the subject of appeal in the Third Circuit.[130] In a rare showing of solidarity, the opinion was also signed by four other magistrate judges.[131] Judge Lenihan's decision found that historical CSLI could not be obtained without a showing of probable cause.[132] That opinion and other historical CSLI decisions that found a showing of probable cause was necessary first concentrated on the tracking device exception to the definition of electronic communication under 18 U.S.C. § 3117.[133] Some of these cases concluded that historical CSLI was information from a tracking device and therefore

126. *See Suarez-Blanca*, 2008 WL 4200156 at *8–9.

127. *Id.* at *8 n.7.

128. *See id.* at *8–9.

129. *Id.* at *11.

130. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, (W.D. Pa. 2008), *vacated* 620 F.3d 304 (3d Cir. 2010).

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

132. *Id.*

133. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308-09 (3d Cir. 2010), *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 577 (W.D. Tex. 2010).

unobtainable under § 2703(c)(1).[134] The application of § 3117 to historical CSLI is discussed in Part II.A.3 but continues to be litigated in courts.[135]

Other pro-warrant historical CSLI cases found the prolonged surveillance doctrine of *Maynard* persuasive in two contexts. First, that *Knotts* is not dispositive on the issue of prolonged location tracking, and second, that a cell phone user has a reasonable expectation of privacy in his or her continuous movements over the course of a prolonged period of time.[136] However, there are still other cases that found that historical CSLI is obtained under the assumption of the risk doctrine.[137]

3. Third Circuit: The Sliding Scale Compromise

Recently, the Third Circuit became the first United States Court of Appeals to address the issue of whether historical CSLI is obtainable under the SCA, and under what standard of proof.[138] Rather than find that either a section (d) order or a warrant obtainable under a probable cause

---

134. *See In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 575 (W.D. Tex. 2010).

135. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308–09 (3d Cir. 2010); *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 571 (W.D. Tex. 2010).

136. *See In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897, 2010 WL 5437209, at *1 n.3 (E.D.N.Y. Dec. 23, 2010); *In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 838 (S.D. Tex. 2010); *see also In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 581–82 (E.D.N.Y. 2010), *rev'd*, (Nov. 29, 2010) (discussing in greater detail the application of the prolonged surveillance doctrine to historical CSLI by Judge Orenstein).

137. *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); United States v. Navas, 640 F. Supp. 2d 256, 264 (S.D.N.Y. 2009), *rev'd in part*, 597 F.3d 492 (2d Cir. 2010).

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

standard was sufficient, the court found that § 2703(d) created a "sliding scale" by which a magistrate judge could, at his or her discretion, require the government to obtain a warrant or a section (d) order.[139] The court began by analyzing the language of § 2703(d), which states that a "'court order for disclosure under subsection (b) or (c) *may* be issued by any court . . . and *shall* issue *only if* the intermediate [section (d)] standard is met."[140] The court found that the language "may issue" implied court discretion and that this implication was strengthened by the language "only if," in the same sentence.[141] The court reasoned that the words "only if" described a necessary, not sufficient, condition such that a showing of "specific and articulable facts" was necessary, but not automatically sufficient to grant a request for historical CSLI.[142]

In addition, the court avoided the issue of whether historical CSLI was information from a tracking device under 18 U.S.C. § 3117 and therefore exempt from the definition of an "electronic communication" by classifying the data as derived from a "wire communication," which does not have the same tracking device exception.[143] The Court reasoned historical CSLI requested by the government consisted of "records of information collected by cell towers when a subscriber makes a cellular phone call" and that the "historical record is derived from 'wire communication' and does not constitute an 'electronic communication.'"[144]

Further, the court examined the legislative history of CALEA, the SCA and, more specifically, the testimony of Louis Freeh, and found that such testimony did not preclude providing CSLI under a section (d) standard.[145] The court

139. *Id.* at 319.

140. *See id.* at 315 (emphasis in original).

141. *Id.* at 315–16.

142. *Id.* at 316. The example given by the court is "a team may win the World Series *only if* it makes the playoffs;" a team meeting the necessary condition to winning the World Series, making the playoffs, does not guarantee that the team will win the World Series. In contrast, "a team will make the playoffs *if* it wins its division;" *Id.* ("[W]inning the division is a sufficient condition to making the playoffs because a team that wins the division is ensured a spot in the playoffs.").

143. *Id.* at 313.

144. *Id.* at 310.

145. *In re* Application of the United States of America for an Order Directing

instead found that the legislative history and Freeh's testimony supported the notion that the new standard in 1986 was an intermediate standard.[146] The court reasoned that Freeh's testimony focused on the government's ability to obtain the information through a pen register or trap-and-trace device, which was governed by a different, and lower standard than a section (d) order.[147]

One of the most important developments to come out of the Third Circuit's decision was the court's outright rejection of the assumption of the risk doctrine. The Court stated that "[a] cell phone customer has not voluntarily shared his location information with a cellular provider in any meaningful way," reasoning that "it is unlikely that cell phone customers are aware that their cell phones providers *collect* and store historical location information."[148] However, the court ultimately did not find that there were sufficient facts to implicate the privacy of the home and thereby require a warrant under *Karo*.[149] "There is no evidence in this record that historical CSLI, even when focused on cell phones that are equipped with GPS, extends to that realm [of the interior of the home]."[150] Therefore, the court declined to find that historical CSLI by definition, required a probable cause showing in order to be obtained by law enforcement.[151]

II. ANALYSIS: IS A WARRANT REQUIRED TO OBTAIN HISTORICAL CELL-SITE LOCATION INFORMATION?

A. Statutory Framework: How is Cell-Site Location Information Classified and is a Section (d) Order Sufficient

Currently the SCA is out of date and contains internal contradictions.[152] Unclear legal standards, highlighted by the

---

a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010).

146. *Id.*

147. *Id.*

148. *Id.* at 317.

149. *See id.* at 312.

150. *Id.* at 312–13.

151. *Id.* at 313.

152. *See id.* at 319; *September Hearings*, *supra* note 19, at 125 (Statement of James X. Dempsey, Esq., V.P., Center for Democracy and Technology).

Third Circuit's "sliding scale" compromise,[153] have led to confused magistrate judges attempting to interpret the statute, uncertain standards for government access to the information, and resources wasted on litigation of the issue.[154]

1. *Section 2703(d) "Sliding Scale": Is a Showing of Specific and Articulable Facts Enough?*

As stated in Part I.E.3, the Third Circuit found that § 2703(d) contained a "sliding scale" standard of proof whereby a judge or magistrate was permitted but not *required* to grant a request for historical CSLI under a section (d) order.[155] Focusing on the word "may," the court and other advocates of this interpretation argue that the "sliding scale" is a "permissive" reading of § 2703(d), required by the statute's plain language, the rule of constitutional avoidance, and Congress' intent to provide courts with a statutory "safety-valve" to avoid issuing orders that may violate the Fourth Amendment.[156] Advocates of this interpretation argue that the statute contains the words "shall . . . only if" rather than simply "shall . . . if," which must mean that a showing of "specific and articulable facts" is necessary, not sufficient.[157] Otherwise, the statute would read: "[A] court order for disclosure . . . *may be* issued by any court that is a court of competent jurisdiction and *shall* issue *only if*" the [section (d)]

---

153. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 316 (3d Cir. 2010).

154. *See September Hearings*, *supra* note 19, at 125 (Statement of James X. Dempsey, Esq., V.P., Center for Democracy and Technology).

155. *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 316 (3d Cir. 2010).

156. Brief for Elec. Frontier Found. et al. as Amici Curiae Supporting Affirmance of the Dist. Ct. at 14. *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No.08-4227), 2009 WL 3866619 at *6. The doctrine of constitutional avoidance states that where there are two possible readings of the statute, one of which could raise Fourth Amendment concerns, the other must be adopted so long as a reading of the statute is not plainly contrary to the intent of Congress. *See* Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1337 (2008).

157. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315–16 (3d Cir. 2010).

standard is met.[158] According to this view, in order for the word "only" to have meaning, it must be permissive and not mandatory.[159]

The government and other advocates that believe a showing of "articulable facts" is sufficient concentrate on the word "shall."[160] First, advocates of this interpretation emphasize that the plain and unambiguous meaning of the statute should control.[161] Further, advocates argue that § 2703(d) does not mention, or even imply, that a probable cause determination may be required.[162] Therefore, all that is required under § 2703(d) and the plain meaning of the statute is a showing of "specific and articulable facts."[163]

Next, these advocates state that the word "shall" is the language of mandate,[164] and that any other reading emphasizing "may issue" in turn makes the words "shall issue" superfluous.[165] Lastly, these advocates state that the "sliding scale" permissive reading of the statute ignores the overall purpose of section (d)—to allow the government to obtain non-content customer information without having to show probable cause.[166]

In its opinion, the Third Circuit admitted that there is an "internal contradiction" in the statute and asked Congress to remedy the contradiction:

> [W]e are stymied by the failure of Congress to make its intention clear. A review of the statutory language suggests that the Government can proceed to obtain records pertaining to a subscriber by several routes, one being a warrant with its underlying requirement of

158. *See id.* at 315.

159. *See* Brief for Elec. Frontier Found., *supra* note 156, at *1–3.

160. *See* Gov't Reply Brief at 8, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Ser. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No.08-4227), 2009 WL 3866620 at *10.

161. *See* Brief for the United States at 23, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Ser. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No.08-4227), 2009 WL 3866618.

162. *Id.*

163. *Id.*

164. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315–16 (3d Cir. 2010).

165. Gov't Reply Brief, *supra* note 160, at *12.

166. Brief for the United States, *supra* note 161, at *23.

> probable cause and the second being an order under §2703(d). There is an inherent contradiction in the statute or at least an underlying omission.[167]

This debate highlights the need for legislative change in the text of the statute. Whether the legislature intended for a statutory "safety valve," or instead intended for a section (d) standard to be sufficient, that intention should be made clear.

2. Wire Communication vs. Electronic Communication: What Kind of Information is Cell-Site Location Information?

A determination of whether historical CSLI is a wire communication or an electronic communication has serious consequences.[168] Under § 3117, if historical CSLI is classified as an electronic communication, the data could be excluded from disclosure under § 2703(c)(1) because an electronic communication, as defined by the SCA, cannot be information derived from a tracking device.[169] The problem is that historical CSLI could qualify as either a wire or an electronic communication.

There are several reasons why historical CSLI could qualify as a wire communication. First the definition of wire communication in the SCA includes the transmission of the human voice,[170] whereas the definition of electronic communication does not.[171] Further, because historical CSLI requests consist of records of information collected by cell towers when a user makes a phone call, the historical data derives from a wire communication.[172] The legislative history of the definition of wire communication also bolsters this

---

167. *In re* Application of the United States of America 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).

168. *See supra* Part I.C–I.C.1. (discussing the exclusion of data from the definition of "wire communication" if that data can be classified as information derived from a tracking device under 18 U.S.C. § 3117).

169. 18 U.S.C. § 3117 (2011).

170. Brief for the United States, *supra* note 161, at 17, n.13; 18 U.S.C. § 2510(1) (2011).

171. *See* Brief for the United States, *supra* note 161, at 17, n.13; 18 U.S.C. § 2510(12) (2011).

172. *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 (3d Cir. 2010).

argument: "cellular communications—whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone—are included in the definition of 'wire communications' and are covered by the statute."[173]

However, CSLI could also qualify as an electronic communication. An electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio. . . ."[174] Therefore, it is possible that CSLI is an electronic communication because it is not transmitted by "by the aid of *wire, cable, or other like connection.*"[175]

While the specific language in the definition of electronic communication appears persuasive, it ignores the legislative intent of the definition of wire communication to include *all* cellular communications in the definition of wire communication.[176] This Comment's proposal, to separate the standard of proof for historical CSLI between "active use" and "idle use," would help to clarify the distinction between wire communication and electronic communication. Data transmitted *during* a call would constitute an "aural transfer" and would more comfortably fit within the definition of "wire communication."[177] On the other hand, idle use data, data transmitted by the network while the phone is idle, would more comfortably fit the definition of electronic communication.[178]

3. Section 3117 Tracking Device: Is Your Cell Phone a Tracking Device?

If CSLI is classified as an electronic communication under 18 U.S.C. § 2510(12) it must be determined whether a cell phone is a tracking device as defined by § 3117. If so, CSLI would be excluded from the definition of electronic

173. S. Rep. No. 99-541, at 11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565 [hereinafter *CALEA Hearings*].

174. 18 U.S.C. § 2510(12) (2011); *see also* Chamberlain, *supra* note 14, at 1757 n.72.

175. 18 U.S.C. § 2510(1) (2011); *see also* Chamberlain, *supra* note 14, at 1757 n.71.

176. *See CALEA Hearings*, *supra* note 173, at 11.

177. *See* 18 U.S.C. § 2510(1) (2011).

178. *See* 18 U.S.C. § 2510(12) (2011).

communication and therefore would not obtainable under § 2703(c)(1).[179] Perhaps best representing the belief that historical CSLI is excluded from disclosure under the SCA as information derived from a tracking device is Judge Andrew W. Austin who stated: "The bottom line is that cell phones undoubtedly have become 'electronic . . . device[s] which permit[] the tracking of the movement of a person or object.' They *are* tracking devices."[180] Even if one does not feel as strongly as Judge Austin, the definition of a tracking device as stated in the *CALEA hearings* in 1986, is very broad:

> These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.[181]

In the above definition, there are no specific requirements regarding the accuracy of the device.[182] Further, a device is covered under the above definition even if it was not intended or designed to track a person's movements.[183]

However, upon examination of the language of the statute and the traditional uses of a tracking device at the time the statute was enacted a cell phone may not qualify as such a device under § 3117.[184] A true tracking device is

---

179. *See supra* Part I.C–I.C.1. (discussing the exclusion of data from the definition of "wire communication" if that data can be classified as information derived from a tracking device under 18 U.S.C. § 3117).

180. *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 580 (W.D. Tex. 2010).

181. *CALEA Hearings*, *supra* note 173, at 10.

182. *See id.*

183. *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 578 (W.D. Tex. 2010).

184. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308–09 (3d Cir. 2010); *see also June Hearings*, *supra* note 10, at

unknown to, and cannot be disabled or turned off by, the person being tracked.[185] Also, subsection (a) of § 3117 states: "If a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device . . ."[186] and refers to a tracking devices surreptitiously installed by the government, not devices already carried by the user.[187] Judges and commentators argue that the § 3117 exception to the definition of electronic communication applies only to those entities that explicitly provide tracking device services.[188] Once an entity is a "provider of electronic communications" it must provide "records or other information" pertaining to its subscribers or customers,[189] and entities that provide tracking device services in addition to other communications services are obliged to provide location data when the statutory prerequisites of § 2703 are met.[190] Other commentators argue the language of § 3117 above, indicating that a "warrant or *other order*"[191] is required, implicitly authorizes the use of a section (d) order to acquire historical CSLI.[192] Because the application of § 3117 is unclear, courts have sought guidance from the legislature history of the statute.

4. Legislative History: The Scope of § 3117

Courts have analyzed the legislative history of § 3117 and more specifically Director Freeh's testimony discussed in

---

73–74 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

185. *See In re* Application of The United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 681 (W.D. La. 2006).

186. 18 U.S.C. § 3117(a) (2011) (emphasis added).

187. *See June Hearings*, *supra* note 10, at 73–74 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP); *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006).

188. *See June Hearings*, *supra* note 10, at 73–74 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

189. 18 U.S.C. § 2703(c) (2011).

190. *See June Hearings*, *supra* note 10, at 74 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

191. 18 U.S.C. § 3117(a) (2011) (emphasis added).

192. *See In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006).

Part. I.C.2. On one hand, the 1994 Amendments to the SCA raised, rather than lowered, the standard of proof required to access non-content location information.[193] This could constitute the intent of Congress to prevent disclosure of location information except under a probable cause standard.[194] On the other hand the Third Circuit, found that in 1994—when the standard of proof required to obtain "call setup information" was raised—Director Freeh was discussing the standard of proof required for a pen register or trap-and-trace device, which is a lower standard than that for a section (d) order.[195] Because Director Freeh was discussing a lower standard of proof than a section (d) order, by discussion of raising the standard of proof from its existing requirements, Freeh was referring to raising the standard to an intermediate standard—a section (d) order.[196] This is a strong argument for which those advocates of a probable cause standard do not have a response. Overall, it does not appear that the tracking device definition contemplated a cell phone or CSLI, a device that does not have to be installed, but rather contemplated the "beepers" used in *Knotts* and *Karo*.[197]

Even if a court finds that historical CSLI is obtainable under the SCA, the court must also determine if that information is obtainable without a warrant under the Fourth Amendment.

B. Fourth Amendment: Does a Cell Phone User Have a Reasonable Expectation of Privacy in His Cell-Site Location Information?

The majority of Fourth Amendment precedent concerning privacy and law enforcement surveillance was decided before the advent of devices like cell phones, which are deeply

193. *See In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site Info., 402 F. Supp. 2d 597, 601 (D. Md. 2005).

194. *See* Chamberlain, *supra* note 14, at 1780–81.

195. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010).

196. *Id.*

197. *See* United States v. Karo, 468 U.S. 705, 705 (1984); United States v. Knotts, 460 U.S. 276, 276 (1983).

integrated into our daily lives.[198] Location data generated by a cell phone does not comfortably fit into any Fourth Amendment line of cases: it is difficult to simply label the data "records" under the assumption of the risk doctrine, or to call a cell phone just a tracking device under *Knotts* or *Karo*.[199] In fact, a cell phone is all of the above; it is a unique device that allows a user's movements and approximate location to be recorded, but at the same time generates data that is stored by a third party provider in the ordinary course of business.

1. Is There a Search Under Katz*?*

In order for the Fourth Amendment to be implicated in law enforcement requests for historical CSLI, there must first be a search within the meaning of *Katz*: did the person have an actual subjective expectation of privacy, and was that expectation one that society is prepared to recognize as objectively reasonable?[200] Because CSLI is "hidden, continuous, indiscriminate and intrusive" most cell phone users are unaware that CSLI is being collected by CSPs, but if they were, they would have a subjective expectation of privacy in this information.[201]

From an objective standpoint, society holds special privacy expectations for telephones, including cell phones, and those expectations extend to historical CSLI.[202] The

198. *See Karo*, 468 U.S. at 705; *Knotts*, 460 U.S. at 276; Katz v. United States, 389 U.S. 347, 347 (1967) (Harlan, J., concurring).

199. *See infra* Part II.B.3 (discussing the problems in analyzing data gleaned from a cell phone under the *Knotts*/*Karo* distinction).

200. *Katz*, 389 U.S. at 361 (Douglas, J., concurring).

201. Brief for Susan Freiwald as Amici Curiae Supporting the Dist. Ct. at 8–9, *In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2008 WL 3861766; *see In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 576 (W.D. Tex. 2010); *see also In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 592-93 (E.D.N.Y. 2010).

202. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010); *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 587 (E.D.N.Y. 2010).

Supreme Court in *Katz* based constitutional protection of telephone calls on the overriding importance of the telephone: "whatever people actually thought or knew about the privacy of their telephone calls, they were *entitled to believe* in the privacy of those calls, because any other result would be destructive of society's ability to communicate."[203] Simply because the phone company or law enforcement could access historical CSLI, the privacy expectation is not diminished—there is an expectation that those parties will not do so as a matter of course.[204]

On the other hand, cell phone users, through experience, subjectively know that their location is disclosed to the CSP.[205] "Any cell phone user who has ever had a call dropped due to a lack of service knows that their cell phone communicates with the nearest tower."[206] In addition, the Supreme Court has always assumed a high degree of awareness in the American public and thus, a lack of expectation of privacy—evidenced by the lack of reasonable expectation of privacy in such technologies as helicopter fly-overs and high-powered cameras.[207]

In *Katz* the Supreme Court emphasized a content/non-content distinction in an objective expectation of privacy, and in *Katz*, it was the content of the communication which enjoyed an objective expectation of privacy, not the record associated with the phone call.[208] As location-based cell phone services grow, public awareness of those services will grow as well, and the expectation of privacy will diminish accordingly.[209]

---

203. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 29 (2007).

204. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010).

205. *See In re* Application of The United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 681 (W.D. La. 2006).

206. *Id.*

207. *See* McLaughlin, *supra* note 13, at 435. The Supreme Court found that there was not an expectation of privacy with respect to helicopter fly-overs in Florida v. Riley, 488 U.S. 455 (1989) and high power cameras in Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

208. Katz v. United States, 389 U.S. 347, 361–362 (1967) (Harlan, J., concurring).

209. *See* McLaughlin, *supra* note 13, at 439–40.

Altogether, it is important to note that the *Katz* test for a search has been criticized for both its circular reasoning and the unfettered discretion it gives to judges in deciding whether society objectively finds an expectation of privacy reasonable.[210] Presumably, all defendants will assert that they had a subjective expectation of privacy, which, in effect, turns the entire *Katz* analysis into an evaluation of whether that expectation was objectively reasonable.[211] However, Courts have not created a method to determine whether society deems an expectation of privacy to be reasonable or not.[212] Further, if *Katz* is taken to its logical conclusion, the government could simply diminish reasonable expectations of privacy by "announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance."[213]

Recent case law such as *United States v. Maynard* shows how an individual can have a reasonable expectation of privacy in non-content information like GPS data (or historical CSLI) that is continuously gathered over a prolonged period of time.[214] The content/non-content distinction of *Katz* is not as useful when the non-content information gathered over an extended period of time has the potential to reveal an intimate picture of the user's life.[215] Instead, this Comment proposes a reasonable expectation of privacy distinction based on whether the user has actively generated data that could convey his location through control of his phone or if the phone has generated the data without any activity or control by the user.

---

210. Freiwald, *supra* note 203, ¶ 21. Having the word "reasonable" in both the name of the test and its definition has prompted some to criticize the test as circular: reasonable expectations are reasonable. *Id.* ¶ 21.

211. *Id.* ¶ 22.

212. *Id.* ¶ 23.

213. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

214. United States v. Maynard, 615 F.3d 544, 563 (2010), *reh'g en banc denied sub nom.*; United States v. Jones, 625 F.3d 766 (2010), *cert. granted* 131 S. Ct. 3064.

215. *Id.*

2. Assumption of the Risk: Has a Cell Phone User Voluntarily Conveyed His Location?

In addition to the *Katz* analysis, courts must also determine whether historical CSLI is obtainable under the assumption of the risk doctrine. If a cell phone user is found to have voluntarily conveyed historical CSLI to a CSP, and therefore assumed the risk that his CSLI could be conveyed to law enforcement, that cell phone user would not have a legitimate expectation of privacy in his historical CSLI.[216]

Because CSLI is generated automatically by the CSP network, the voluntary decision to use a cell phone cannot be equated with the voluntary conveyance of idle CSLI.[217] Further, the "choice" to use a cell phone in today's society is really no choice at all, as many individuals are required to carry cell phones for work or other legitimate purposes.[218] In addition, the substance of the records of CSLI are different from the records voluntarily conveyed in *Miller* and *Smith* in that the information is collected without the user's knowledge, and the data provides the ability to track the user's movements on a relatively precise and continuous basis.[219] This is in contrast to other records accessible under the assumption of the risk doctrine (e.g. credit card, ATM, electronic toll collection systems) where it is clear to the person engaging in the transaction that the transaction was being recorded, and that transaction was only a specific moment in time.[220]

At the same time, historical CSLI is a record or other information which is voluntarily conveyed to the CSP by virtue of the use of the cell phone, leading some courts to conclude that the user thereby assumes the risk that the CSPs will create its own internal record and turn over this information to the government.[221] This argument focuses on

---

216. Smith v. Maryland, 442 U.S. 735, 735 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

217. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010).

218. Chamberlain, *supra* note 14, at 1786.

219. *See June Hearings*, *supra* note 10, at 69–70 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

220. *See id.*

221. *See* United States v. Velasquez, No. CR 08-0730, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (analogizing to *Pineda-Moreno*); Brief for the United

the fact that cell phone records are maintained in the course of business, and, just like any other business, individuals do not have a subjective expectation of privacy in those records.[222] In addition, other records, such as detailed bank and electronic commuter pass records that reveal the location of the consumer, are ordinarily obtainable with a court order.[223]

The assumption of the risk doctrine fits comfortably within the framework proposed by this Comment. If the phone is in active use, the CSLI accompanying that call is transmitted on the same frequency as the call itself and is information voluntarily conveyed to the phone company.[224] In addition, when a user makes a call or answers a call he or she knows that that they have conveyed their location information in order to complete the call. As the one court has insightfully stated, anyone who has had a call dropped knows that his cell phone communicates with the nearest cell tower.[225] An implicit assumption in the knowledge that your cell phone is communicating with the nearest tower is that the cellular network knows the location of your phone, because it knows the location of the tower that your phone is communicating with. Thus, when a cell phone user makes or receives a call, and knows that his phone is communicating with the nearest cell tower, he is aware that he has conveyed his approximate location to the CSP. Further, similar to a credit card or electronic toll collection service,[226] it is clear to the person generating active use data that the data is being recorded (for billing purposes) and the transaction occurred in

---

States, *supra* note 161, at *28.

222. *See* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8–9 (N.D. Ga. Apr. 21, 2008).

223. *See June Hearings*, *supra* note 10, at 61–62 (statement of Richard Littlehale, Assistant SAC, F.B.I.).

224. *See* McLaughlin, *supra* note 13, at 426.

225. *See In re* Application of The United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 681 (W.D. La. 2006).

226. An electronic toll collection service provides an electronic pass that the user carries in his or her vehicle to automatically pay the toll as the vehicle passes through the toll booth. *Electronic Toll Collection Systems*, U.S. GENERAL SERVICES ADMINISTRATION, http://www.gsa.gov/portal/content/104326.

only a specific moment in time.[227] Because the cell phone user has voluntarily conveyed his location information to the CSP through the conscious physical act of making or receiving a call, he has assumed the risk that his location information could be turned over to law enforcement.

Idle CSLI however, truly is information that is silently collected as an "automatic byproduct" of cell phone service and recorded without any affirmative act by the cell phone user, except that of turning the cell phone on.[228] If the user wants to enjoy the purpose of his cell phone, to be able to make or receive calls, he must leave the phone on. Further, most, if not all cell phone users are unaware that the cellular network is calculating their location information, because they have not taken any affirmative steps to convey that location to the CSP. Under these circumstances a cell phone user has not voluntarily conveyed this information to the CSP and has an objective expectation of privacy in his or her historical CSLI.

3. Electronic Surveillance: The Beeper Cases

The Supreme Court established through its decisions in *Knotts* and *Karo* that the use of a beeper requires a warrant when private spaces (usually the home) are implicated, but not when the device is used to track a suspect's movements in public areas.[229] But, how important is the home/public spaces distinction when the "tracking device" is also a phone? Under a strict reading of *Karo*, if historical CSLI may at times be accurate enough to implicate the home, historical CSLI requests should always require a warrant.[230]

> If an intrusion into a legitimate expectation of privacy takes place only once, or in limited bursts, it is still an intrusion, and it still requires probable cause under the

227. *Cf. June Hearings*, *supra* note 10, at 69–70 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

228. *See* McLaughlin, *supra* note 13, at 426.

229. *See* United States v. Karo, 468 U.S. 705, 715 (1984); United States v. Knotts, 460 U.S. 276, 281 (1983).

230. *See In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 579 n.15 (W.D. Tex. 2010).

> Fourth Amendment . . . there is nothing in any of the relevant statutes that makes a distinction between limited location information and fully robust, minute-by-minute location information.[231]

Further, the uncertain nature of the accuracy of CSLI could require a warrant to avoid a constitutional violation, because the suspect may be unintentionally tracked in a private location.[232] In addition, even if CSLI is not dependably accurate, a user who lives in a "palatial estate" still may have their privacy infringed if CSLI is accurate within even 100 yards.[233] Further, as CSLI becomes increasingly accurate,[234] 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.[235]

However, currently 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.[236] *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.[237] In *Karo*, in an incident separate from the agents' use of the beeper to discover that ether was located inside the home of the defendant, the beeper was used to discover that the ether was located somewhere in a storage

---

231. *Id.*

232. *See* McLaughlin, *supra* note 13, at 441–42.

233. Chamberlain, *supra* note 14, at 1788.

234. *See supra* Part I.A.2 (discussing the increasing accuracy of CSLI as technology develops and more and more cell towers are erected).

235. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 836 (S.D. Tex. 2010).

236. *See In re* Application of the United States of America for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010) (concluding there were insufficient facts to implicate *Karo*); *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 80–81 (D. Mass. 2007) (concluding that historical CSLI reveals nothing more than what could be gleaned from a pen register); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info., 622 F. Supp. 2d 411, 418–19 (S.D. Tex. 2007) (finding that there was no risk of improper tracking for data from a single tower antenna).

237. *See* Brief for the United States, *supra* note 161, at 29.

facility.[238] However, the beeper only indicated that the ether was somewhere in the facility, it did not indicate the specific locker where the ether was located.[239] It was only after the agents used their sense of smell as they walked around the facility that they were able to detect in which storage container the ether was located.[240] The Court found that this use of the beeper did not violate the Fourth Amendment because the beeper did not reveal anything about the contents of the storage locker and hence was not a search of the locker.[241] This situation is similar, if not identical, to using CSLI to discover whether the suspect is in or near his home.[242]

In addition, unlike in *Knotts* and *Karo* the alleged tracking device is not just a tracking device, but also a phone, and analogous to *Smith v. Maryland* and a pen register or trap-and-trace device.[243] When a trap-and-trace device is installed in a suspect's home phone, the suspect's general location will be disclosed every time the phone is in use.[244] The government may not know where the suspect is within the home, but they will know that he (or someone in his home) is dialing from his home phone.[245]

The analogy of a CSLI to a pen register seizes on an important distinction between the devices used in *Knotts* and *Karo*, and a cell phone. An emphasis on the privacy of the home makes sense in the context of a tracker beeper that has no other uses except as a tracking device, but it makes less sense in the context of a device that has other functions, such as making phone calls, which might also be used to determine the location of a suspect. There is little if any difference

238. United States v. Karo, 468 U.S. 705, 720 (1984).
239. *Id.*
240. *Id.* at 720–21.
241. *See id.*
242. *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007); Brief for the United States, *supra* note 161, at 29.
243. *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007).
244. *Id.*
245. *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007).

between determining that a suspect who lives alone is home when he uses his landline through a pen register or trap and trace, and determining that he is located within the home when he makes a call from his cell phone. While there is a reasonable expectation of privacy in the interior of the home, there is not a reasonable expectation of privacy in everyday manifestations that are observable from the street[246] or from records that the party has assumed the risk will be conveyed to law enforcement.[247] These observations or records can just as easily indicate whether or not a party is home.

In addition, unlike the tracker beepers in *Knotts* and *Karo*, which indicated where an inanimate object was located in the home,[248] law enforcement use of historical CSLI to determine whether a suspect is at home is no different from the use of other external manifestations which do not require a warrant. In *Karo* the police were not attempting to discover if the suspect was at home, they were attempting to discover whether the suspect had something within his home.[249] This is in contrast to the use of historical CSLI to determine whether a suspect is at home—law enforcement is not concerned with what is taking place or contained in the interior of the home, only that the suspect is there. If, however, law enforcement uses historical CSLI to pinpoint where a suspect is located within the interior of his home, this use would violate the user's reasonable expectation of privacy because traditional call data cannot be used for this purpose and neither can surveillance technologies without a warrant.[250]

Further, in the context of the warehouse in *Karo*, there should not be a difference in Fourth Amendment protection for an individual who lives in a small, dense housing area, and one who lives in a "palatial estate."[251] However, as it currently stands, the suspect who lives in the dense housing area—where CSLI might indicate that he is at home or it

246. United States v. Karo, 468 U.S. 705, 714 (1984).
247. Smith v. Maryland, 442 U.S. 735, 744 (1979).
248. *Karo*, 468 U.S. at 714.
249. *Id.*
250. *See id.*
251. *Compare* Chamberlain, *supra* note 14, at 1788 *with* United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010), *reh'g en banc denied,* 617 F.3d 1120, 1123 (9th Cir. 2010).

might indicate that he is in the common area of the complex (with no reasonable expectation of privacy)—and the suspect in the palatial estate—where the information would likely indicate that he was in the interior of his home—would have different Fourth Amendment standards apply.[252] 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. Additionally, in *United States v. Maynard*, the Court found that the duration of the tracking is not addressed by the *Knotts* and *Karo* cases, which has become an important emerging issue.[253]

4. Prolonged Surveillance Doctrine

The prolonged surveillance doctrine announced in *United States v. Maynard*[254] has recently been adopted by courts discussing CSLI and has offered an alternative analysis to the *Knotts*/*Karo* distinction.[255] As stated in the June Congressional hearings:

> I mean, if I am continuously tracked everywhere I go all day, the fact that sometimes I am outside and sometimes I am inside doesn't give me comfort that it was okay to track me during those moments I was outside . . . .
>
> It is not were you in the house at that moment? It is are we learning something about your continuous movement versus learning something about you at a given moment in time . . . .[256]

Advocates of the prolonged surveillance doctrine argue that the longer an investigation runs, the more likely that

252. *See* Chamberlain, *supra* note 14, at 1788. If the defendant were in a small dense area where the CSLI might only indicate that he was within the area of the apartment, this would appear to fall within the scenario of the warehouse in *Karo*, whereas if the defendant were in a large palatial estate, this would appear to fall within the holding of *Karo* and be an impermissible search. *See Karo*, 468 U.S. at 720.

253. *See infra* Part II.B.4 (discussing the implications of the prolonged surveillance doctrine on CSLI jurisprudence).

254. United States v. Maynard, 615 F.3d 544, 544 (2010), *reh'g en banc denied sub nom.*; United States v. Jones, 625 F.3d 766 (2010), *cert. granted* 131 S. Ct. 3064 (2011).

255. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 836–37 (S.D. Tex. 2010).

256. *June Hearings*, *supra* note 10, at 98 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

investigation will intrude upon a suspect's privacy.[257] Further, they argue that the continuous nature of the surveillance distinguishes it from traditional methods used to track a suspect's movements, such as purchase receipts and banking records or even police surveillance.[258]

Opponents of the prolonged surveillance doctrine point out that there are differences between the facts of *Maynard* and CSLI that warrant attention. In *Maynard*, GPS, a more accurate technology, was used to track the suspect and allowed for greater precision.[259] In *Maynard*, the tracking device was attached to the suspect's car, and was therefore on public roadways through almost the entirety of the "surveillance," and the suspect's movements were tracked in real time.[260] In addition, one opponent of the prolonged surveillance doctrine stated: "Although continuous monitoring may capture quantitatively more information than brief stints of surveillance, the type of information collected is qualitatively the same."[261]

Further, the prolonged surveillance doctrine has been criticized for the vagueness that the doctrine introduces.[262] At what point does surveillance become so prolonged as to have crossed the line into a Fourth Amendment violation?[263] What effect might this doctrine have on police visual surveillance, for which a warrant is not required?[264]

The difference between the GPS used in *Maynard* and CSLI, however, do not go to the heart of the issue: the *duration* of tracking and the entire picture of the suspect's life

257. Freiwald, *supra* note 203, ¶ 69.

258. *See June Hearings*, *supra* note 10, at 98 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

259. *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 589 n.13 (E.D.N.Y. 2010).

260. *See id.* at 595.

261. United States v. Sparks, 750 F. Supp. 2d 384, 392 (D. Mass. 2010).

262. *See id.*

263. *See id.*; *cf. In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 11-MC-0113, 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011) (finding that while such line drawing is arbitrary, the need for such arbitrariness and its application is nothing new for law enforcement officers seeking to perform their duties without running afoul of their targets' constitutional rights).

264. *See id.*; United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010), *reh'g en banc denied*, 617 F.3d 1120 (9th Cir. 2010).

learned from that tracking.[265] In addition, while the logistical problems of the prolonged surveillance doctrine are real, the point that it makes about the intrusiveness of "whole picture" is also very real. By examining the whole of a defendant's movements over the course of time, the government is able to learn more about a suspect than they would were he only followed for one day—they learn the intimate pattern of his life.[266] For this reason this Comment advocates that as long as historical CSLI is obtainable in active use under a section (d) order, that the duration of data obtainable be limited in time. Requests for anywhere from sixty to one hundred days are too intrusive into the life of a suspect.[267]

The active/idle use distinction proposed by this Comment would preserve and implement the prolonged surveillance doctrine of *Maynard*. Active use data, obtainable under a section (d) order, would only include the limited instances in which a suspect dialed or received a call. This data, unlike idle use data, is not continuous, as even the most frequent cell phone user is not on his phone twenty-four hours a day. By limiting data obtainable without a warrant to the limited instances where a cell phone user makes or receives a call, in conjunction with a limit on the number of days over which the information can be obtained, this Comment's proposal avoids the prolonged surveillance concerns of *Maynard*.

---

265. *In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 838 (S.D. Tex. 2010).

266. *See* United States v. Maynard, 615 F.3d 544, 544 (2010), *reh'g en banc denied sub nom*; United States v. Jones, 625 F.3d 766 (2010), *cert. granted* 131 S. Ct. 3064 (2011); *see, e.g.*, Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES (Mar. 26, 2011,) http://www.nytimes.com /2011/03/26/business/media/26privacy.html (demonstrating the information that is generated through historical CSLI, including an interactive map).

267. *See, e.g.*, *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 11-MC-0113, 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011); *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897, 2010 WL 5437209, at *1 (E.D.N.Y. Dec. 23, 2010) (reviewing an order requesting historical CSLI for 113 days prior to the date of the order); *In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 841 (S.D. Tex. 2010) (reviewing an order requesting historical CSLI and call detail records for sixty days prior to the date of the Order).

III. PROPOSAL

Technology has outpaced existing statutes and Fourth Amendment Precedent, leading to conflicting legal standards that create uncertainty for law enforcement and courts.[268] In addition, current Fourth Amendment jurisprudence governing the voluntary disclosure of records and other cases governing electronic surveillance does not assimilate well to a device like a cell phone, which both creates ordinary business records and allows for location-based surveillance.[269] This Comment proposes a new legislative and Fourth Amendment distinction: active-use CSLI, data generated when the call is made (or received) and when the call is ended, would be obtainable under a section (d) order; whereas idle CSLI, data generated by the cellular network in order to locate the cell phone if and when a call is made, would be obtainable only under a probable cause standard. This framework comfortably fits within the current existing definitions of the SCA, as the active/idle use distinction helps to resolve the issue of whether historical CSLI is a wire communication or an electronic communication. Active use data, the data generated during the call,[270] qualifies as a wire communication[271] and idle use data fits the definition of an electronic communication.[272] Further, this distinction preserves the existing tracking device exception to electronic communication.[273] Application of the active use framework to the SCA can best be accomplished by legislation mandating that CSPs keep limited CSLI records and unlimited CSLI records separate and distinct. Legislation regulating what kind of location information generated by cell phones can be stored and under what circumstances has been enacted by

268. *See September Hearings*, *supra* note 19, at 1–2; *supra* Part II.A (discussing the problems with the current statutory framework governing historical CSLI disclosure).

269. *See supra* Part II.B.3 (discussing the problems that are encountered when trying to fit CSLI into the *Knotts*/*Karo* analysis).

270. *See supra* note 39 and accompanying text.

271. *See supra* note 74 and accompanying text (stating that a wire communication is an "aural transfer").

272. *See supra* Part II.A.2 (discussing the distinction between wire communication and electronic communication).

273. *See supra* Part II.A.3 (discussing the tracking device exception to the definition of electronic communication).

other governments, most notably the European Union.[274] This legislation can provide the Legislature with a possible model to protect location information.[275]

In addition, the active use framework tries to strike the appropriate balance in current Fourth Amendment precedent. The content/non-content distinction of *Katz* is not useful in the context of historical CSLI when the non-content information generated over a prolonged period of time has the potential to reveal an intimate picture of the cell phone user's life and implicate a reasonable expectation of privacy under *Maynard*.[276] Instead, the active use framework proposes a reasonable expectation of privacy distinction based on whether the user of the phone is actively conveying their location to the CSP by virtue of making or receiving a call, or if the phone has generated data without any control by the user.

The active use distinction also helps to adapt the assumption of the risk framework to historical CSLI jurisprudence. Active use CSLI, those records that the user actively generates by making and receiving calls, is more closely analogous to landline phone records that do not require a warrant under the assumption of the risk framework.[277] However, idle use data which is silently and continuously collected by the cellular network without any action by the cell phone user would require a warrant as it more appropriately falls outside of the assumption-of-the-risk framework.[278]

Also, the active use distinction tries to reconcile the holdings of *Knotts* and *Karo* with the fact that landline phone records can, and do, provide police officers with information regarding a suspect's location. Instead of analyzing a

274. *See* Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37–47.

275. *See June Hearings*, *supra* note 10, at 155–56 (statement of Electronic Privacy Information Center).

276. The Supreme Court has granted certiorari on *Maynard*. The outcome of this decision could greatly shape CSLI jurisprudence as well.

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

278. *See supra* Part II.B.2 (discussing the how CSLI fits into the assumption of the risk framework).

reasonable expectation of privacy based on *where* the user is when the information is collected, this Comment proposes a distinction based on whether the user is actively controlling, or instead if the cellular network is gathering the user's location information while the phone is idle However, if law enforcement uses historical CSLI to pinpoint where a suspect is located within the interior of his home, this use would violate the user's reasonable expectation of privacy under *Karo* because traditional call data or other police surveillance cannot be used for this purpose and neither can other surveillance technologies.[279]

Lastly, this proposal finds the prolonged surveillance doctrine of *United States v. Maynard* persuasive and advocates for legislative changes that would curtail the window of time within which law enforcement could gain access to historical CSLI records, regardless of whether active or idle use.[280] Active use data, obtainable under a section (d) order, would only include the limited instances in which a suspect dialed or received a call. By limiting data obtainable under a section (d) order to instances in which the suspect dials or receives a call, the proposal of this Comment hopes to avoid the prolonged surveillance concerns of *Maynard*.

This proposal strikes the appropriate balance sought by Congress.[281] It balances the privacy of the user in his or her movements when not actively using their cell phone against the needs of law enforcement to build a case and gather information. In addition, this framework provides a bright line rule for courts to follow; no longer must the court speculate how accurate the data is in order to determine whether or not the privacy of the home is implicated, or struggle with a statute that does not mesh with current uses of technology.[282]

---

279. United States v. Karo, 468 U.S. 705, 714 (1984).

280. *See In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 841 (S.D. Tex. 2010) (reviewing an order requesting historical CSLI and call detail records for sixty days prior to the date of the Order).

281. *See supra* notes 19–22 and accompanying text (discussing the goals of Congress in the recent hearings regarding the ECPA and communications technologies).

282. *See supra* Part II (analyzing the problems with the existing statutory framework and Fourth Amendment precedent).

A. Proposed Legislation: Amendments to the ECPA

As stated above, in May 2011 Senator Leahy of the Senate Judiciary Committee introduced a bill in the U.S. Senate to update the Electronic Communications Privacy Act, including the SCA.[283] The proposed legislation, as currently written, would allow law enforcement to obtain historical CSLI under either a search warrant or a section (d) order.[284] A summary of the proposed changes prepared by Senator Leahy states that the new statutory language "codifies the government's current practice for obtaining this kind of location information."[285]

Without more information, the exact implications of allowing law enforcement to obtain historical CSLI under either a search warrant or a section (d) order remain unclear. It is uncertain from the statutory language or the accompanying summary by Senator Leahy if the Third Circuit's ruling that a finding of specific and articulable facts is necessary but not sufficient is still valid. If the government has the necessary proof to meet the specific and articulable facts standard, must the court grant the government's request, or can the court, in its discretion, require law enforcement to obtain a warrant?

Additionally, although the proposed legislation may settle the current disagreement regarding the standard for law enforcement to obtain historical CSLI under the SCA, whether law enforcement is required to obtain a warrant under the Fourth Amendment would still remain unsettled. Recent decisions have denied government requests for historical CSLI not under the SCA, but the Fourth Amendment, either because historical CSLI can be accurate enough to implicate constitutionally protected privacy of the home under *Knotts* and *Karo* or under the prolonged surveillance doctrine of *Maynard*.[286] The proposed legislation

283. Rachelle Dragan, *US Senate Sinks its Teeth into Online Privacy Reform*, TECHNEWSWORLD (July 7, 2011), http://www.technewsworld.com/story/72477.html.

284. Press, Release, Senator Patrick Leahy, *Leahy Introduces Benchmark Bill To Update Key Digital Privacy Law*, SENATOR PATRICK LEAHY (July 16, 2011) http://leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29e3c5f758f2.

285. *Id.*

286. *In re* Application of the United States of America for Historical Cell Site

would not settle these issues and the Fourth Amendment implications of historical CSLI data will likely remain a subject of litigation in courts.

B. Supreme Court Decision in United States v. Jones

The Supreme Court reached a decision in *United States v. Jones* (formerly *Maynard*) shortly before publication of this Comment. The majority opinion, authored by Justice Scalia, held that the Government's installation of a GPS device on the defendant's vehicle and the use of that device to monitor the vehicle's movements was a search within the meaning of the Fourth Amendment.[287] The Court reached this result by replying upon common-law trespass jurisprudence instead of applying the *Katz* analysis.[288]

However, in dicta the Court discussed whether the Government's use of a GPS device to monitor a defendant's movements might also have violated the defendant's Fourth Amendment rights under *Katz*.[289] The small portion of Justice Scalia's majority opinion to discuss this issue focused on the duration of the tracking.[290] Justice Scalia rejected any distinction between short-term and long-term GPS monitoring, stating that such analysis leads to "additional thorny problems."[291]

In his concurring opinion,[292] Justice Alito indicated that under the *Katz* analysis he would hold that "relatively short term monitoring" of a person's movements on public streets

---

Data, 747 F. Supp. 2d 827, 838 (S.D. Tex. 2010); *In re* Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Base Services, 727 F. Supp. 2d. 571, 572 (W.D. Tex. 2010).

287. *United States v. Jones*, No. 10-1259, 2012 WL 171117, at *3 (S. Ct. Jan. 23, 2012)

288. *Id.* at *3–4. The Court in *Jones* stated that "[t]he Government physically occupied private property for the purpose of obtaining information. 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". *Id.* at *3.

289. *Id.* at *7–8.

290. *Id.*

291. *Id.*

292. The bulk of Justice Alito's concurring opinion critiques Justice Scalia's use of common law trespass jurisprudence instead of the Katz analysis to decide the issue. *Id.* at *11–16 (Alito, J., concurring).

do not violate an individual's reasonable expectation of privacy whereas longer term GPS monitoring would.[293] Justice Alito declined to create a standard for how long GPS monitoring must continue until it implicates a suspect's reasonable expectation of privacy, stating that "[w]e need not indentify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[294]

Justice Sotomayor, who joined Justice Scalia's majority opinion but also wrote her own concurring opinion, took the strongest stance on the use of GPS devices to monitor a suspect. Justice Sotomayor stated that she believed even shot-term monitoring could violate an individual's reasonable expectation of privacy.[295] She continued by expressing her belief that the low cost and wide availability of GPS trackers could have such a dramatic effect on American society so as to "chill[] associational and expressive freedoms."[296] Finally, Justice Sotomayor stated 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," on the grounds that the assumption of the risk framework was "ill suited to the digital age in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[297]

While it remains to be seen what the lasting effect of *Jone*s 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 device used to generate location information—the user is already carrying around his or her cell phone.[298] Second, the Court did not explain what level of proof is required to conduct the "search" that occurred in *Jones*.[299] The Court expressly declined to address the Government's argument that the police officers

293. *Jones*, 2012 WL 171117, *17 (Alito, J., concurring).
294. *Id.*
295. *Id.* at *9 (Sotomayer, J., concurring).
296. *Id.*
297. *Id.* at *10
298. *See supra* note 65 and accompanying text.
299. *Jones*, 2012 WL 171117, at *3–8.

had reasonable suspicion or probable cause to conduct the search on the grounds that the argument was not raised below.[300] This has lead at least one commentator to wonder if the Court could later find that the search caused by installing a GPS device requires only reasonable suspicion.[301]

Third, the court has not fashioned any of kind of standard as to when the monitoring of a person's movements begins to impinge upon a reasonable expectation of privacy. Justice Alito's concurring opinion attempts to make a distinction between short-term and long-term GPS monitoring, but then he declines to articulate a standard to differentiate between the two categories. Justice Alito simply states that "the line was surely crossed before the 4-week mark."[302] Until many of the questions left open by *Jones* are answered, the Court's decision may only add to the confusion and lack of clarity that currently persists in historical CSLI jurisprudence. The proposal for this Comment, to distinguish between active and idle use data, could help to provide a more discernable standard for when a warrant is or is not required for law enforcement to obtain historical CSLI records.

CONCLUSION

Cell phones have changed the way that people communicate with each other, but they also generate a wealth of personal information about where we have gone and to whom we have communicated with. The current statutory framework for law enforcement access to historical CSLI is out of date, contains internal contradictions, and is presently the subject of litigation in courts.[303] Additionally, existing Fourth Amendment precedent does not adequately balance the privacy expectations of users with respect to a device that both conveys their location *and* generates records in the ordinary course of business. The result of these shortcomings is that courts have struggled to analogize historical CSLI to

300. *Id.* at *8.

301. Tom Goldstein, *Reactions to Jones v. United States: The government fared much better than everyone realizes*, SCOTUSBLOG (Jan. 26, 2010, 10:20 AM), http://www.scotusblog.com/2012/01/reactions-to-jones-v-united-states-the-government-fared-much-better-than-everyone-realizes/.

302. *Jones*, 2012 WL 171117, at *27 (Alito, J., concurring).

303. *See supra* Part III.

normal business records or to a tracking device, when in fact it is both.

By proposing a new distinction between when the phone is in active use and when it is idle, this Comment hopes to provide a new, unambiguous legal framework that will help provide the legislature and courts with a test that adequately balances the privacy of the cell phone user with the reasonable expectations of society, and law enforcement's need to protect the public. As technology and its uses change, so must our statutes and Fourth Amendment jurisprudence.