PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 39 | Issue 3 Article 4

4-15-2012

The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy

Kyle Malone

The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy

I. INTRODUCTION

On February 6, 2001, Gus Boulis, a well-respected business tycoon, was gunned down in his car in Fort Lauderdale, Florida while driving away from a business meeting.[1] Despite its high profile, the subsequent police investigation suffered from a lack of cooperation[2] and a lack of physical evidence.[3] The prosecutor gathered evidence for four years and finally charged three men with the murder.[4] The three suspects have been awaiting trial for over five years, and a critical point of the pretrial wrangling has focused on the admissibility of two of the suspects' cell phone records.[5] These records are crucial to the case because an analysis of the location data contained in them places two of the men within 500 feet of the murder as it was taking place.[6] However, the defense challenged the admissibility of the records because the police obtained them without a warrant.[7] The defense claimed this action violated defendants' constitutional rights,[8] but on February 24, 2011, a Florida judge refused to suppress the cell phone records, citing federal precedent that indicates cell phone users have no reasonable expectation of privacy in location information gathered by the

1. Paula McMahon, *Judge OKs Crucial Evidence in Boulis Murder Case*, SUN SENTINEL, Feb. 24, 2011, http://articles.sun-sentinel.com/2011-02-24/news/fl-gus-boulis-case-cell-phone-20110224_1_ferrari-and-fiorillo-james-pudgy-fiorillo-anthony-little-tony-ferrari.

2. *See* Jeff Shields & Ardy Friedberg, *Boulis Slaying Investigation Loses Impetus*, SUN SENTINEL, Sept. 27, 2005, http://www.sun-sentinel.com/news/local/southflorida/sfl-927boulisimpetus,0,5933261.story. After questioning Adam Kidan, a former business rival of Boulis, detectives from Fort Lauderdale admitted that they "[didn't] feel he was totally candid with us." *Id.* In addition, roughly a year after the murder, no one had come forward with any information leading to an arrest, despite the fact that a $100,000 reward was available for such information. *Id.*

3. McMahon, *supra* note 1.

4. Barbara Hijek, *Gus Boulis: Life, Violent Death and the Aftermath*, SUN SENTINEL, Oct. 13, 2010, http://articles.sun-sentinel.com/2010-10-13/news/fl-boulis-trial-timeline-20101013_1_james-pudgy-fiorillo-anthony-little-tony-ferrari-kidan-and-abramoff.

5. *See* McMahon, *supra* note 1.

6. *Id.*

7. *Id.*

8. *See id.*

police.[9] The prosecutors in this case saw a major victory in this ruling, but did the privacy rights of all Americans suffer a defeat?[10]

There are approximately 277 million active cell phones in the United States.[11] Beyond the obvious purpose of making calls, newer cell phone models can provide a user with turn-by-turn driving directions, Internet browsing, and even movie rentals.[12] Cell phone owners routinely make calls from locations that, at one time, would have been thought impossible.[13] This technology has become so widespread that cell phones now seem equally indispensable for the average teenager and the traveling businessman.[14] However, some claim that cell phones also represent a serious threat to our constitutional right to privacy.[15] Due in part to the relatively unobtrusive infrastructure of mobile networks,[16] many people probably do not consider how this technology works or what information they may inadvertently be sharing with their cell phone company.

---

9. *Id.*

10. *See id.*

11. Michael Isikoff, *The Snitch in Your Pocket: Law Enforcement Is Tracking Americans' Cell Phones in Real Time—Without the Benefit of a Warrant*, NEWSWEEK, Mar. 1, 2010, at 40.

12. *E.g.*, Alex Colon et al., *Dragon Go! (for iPhone)*, PC MAGAZINE.COM (July 29, 2011), http://www.pcmag.com/article2/0,2817,2389440,00.asp; Sascha Segan, *Motorola Droid 2 (Verizon Wireless)*, PC MAGAZINE.COM (Aug. 13, 2010), http://www.pcmag.com/article2/0,2817,2367795,00.asp.

13. This newfound freedom of communication has had some unintended consequences. For instance, hikers seeking to get away from the hustle and bustle of life in the city might find themselves surrounded by other hikers chatting away on their cell phones. This danger is so prevalent that some hiking guides now outline cell phone usage guidelines as part of their discussion on "trail etiquette." *See, e.g.*, DOUGLAS LORAIN, 100 CLASSIC HIKES IN OREGON: OREGON COAST, COLUMBIA GORGE, CASCADES, EASTERN OREGON, WALLOWAS 14 (2004).

14. A recent study by the Pew Research Center found that seventy-five percent of children between the ages of twelve and seventeen own cell phones. Amanda Lenhart, *Teens, Cell Phones and Texting: Text Messaging Becomes Centerpiece Communication*, PEWREASEARCHCENTER PUBL'NS (Apr. 20, 2010), http://pewresearch.org/pubs/1572/teens-cell-phones-text-messages. This is up from only forty-five percent in 2004. *Id.* While teenagers are probably using cell phones strictly for fun, a study released earlier this year found that an incredible 1.1 billion hours are saved by small businesses alone by utilizing applications on smartphones and tablets. Jan Norman, *Mobile Apps Save Small Firms 1.1 Billion Hours*, THE ORANGE COUNTY REGISTER: BUSINESS (June 6, 2011, 6:00 AM), http://jan.ocregister.com/2011/06/06/mobile-apps-save-small-firms-1-1-billion-hours/59961/. This translates to about $17.6 billion in savings for small businesses (fewer than twenty employees) alone. *Id.*

15. *See* Isikoff, *supra* note 11, at 40.

16. Because few people desire the "visual pollution" of plain, metal cell phone towers, companies construct camouflaged towers that look, at first glance, like trees, flag poles, chimneys, or other more visually appealing items. *The Early Show: Cell Phone Towers in Disguise* (CBS television broadcast Nov. 29, 2009), *available at* http://www.cbsnews.com/video/watch/?id=2214391n%3fsource=search.

Because of the sophisticated nature of mobile communications technology, the location of any cell phone, and presumably its owner, can often be easily determined within a few hundred feet.[17] This location information, generally referred to as cell site location information (CSLI), has become a popular way for the government to combat criminal activity.[18] CSLI has been successfully used to catch murder suspects, drug traffickers, and other criminals.[19] Some see CSLI as a powerful and necessary tool for law enforcement.[20] Privacy advocates, however, find the use of these investigative tactics to evoke "Orwellian images of Big Brother," and believe the practice of gathering such information without a warrant violates the Fourth Amendment.[21]

Courts have not adequately addressed what, if any, constitutional protection CSLI deserves.[22] Courts often distinguish between prospective (also known as "real-time") CSLI and historical CSLI. The former allows law enforcement to track a cell phone's movements in real time, while the latter location information is from some time in the past and is gathered from cell phone records.[23] Most jurisprudence in this area has focused on prospective CSLI, and although there is not a definitive answer on the issue, the acquisition of prospective CSLI by the government is generally thought to require a warrant.[24] This is not the case for historical CSLI, access to which was routinely granted for years to government agencies without a warrant on a showing of less than probable cause.[25] Recently, judicial attitudes seem to be shifting.[26] Much has been written by judges, legal

---

17. *See infra* notes 50–56 and accompanying text.

18. *See* Isikoff, *supra* note 11, at 40. In fact, it is estimated that mobile communications companies are receiving "thousands of [CSLI] requests per month." *Id.* To streamline the process of dealing with this high volume of requests, Sprint Nextel has even admitted that the company has established a dedicated web site for law enforcement officials to log on and obtain CSLI from their offices. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. *See infra* notes 64–69 and accompanying text.

23. *See infra* notes 59–62 and accompanying text.

24. *In re* the Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 595, 601 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010) [hereinafter W.D. Pa. Opinion].

25. *See* Isikoff, *supra* note 11, at 40.

26. Magistrate Judge James Orenstein was the first judge in the country to issue a published opinion denying an order for CSLI (either prospective or historical), and he did so in 2005. *In re* an Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005). This decision marked a significant shift in jurisprudence not only because it was the first published decision denying such an order, but also because as Magistrate Judge Orenstein acknowledged in his opinion, he himself had been routinely granting requests for CSLI as recently as four months before he changed his mind in the instant case. *Id.* at 566. While Magistrate Judge Orenstein did not differentiate between historical and prospective CSLI, see *id.*, it sparked a

scholars, and law students alike arguing that a probable cause standard should be applied to all applications for CSLI—historical or otherwise.[27] Concerns over privacy rights are not confined to judges and academics. Advocacy groups are devoting time and resources to fight for a probable cause standard and legislators are beginning to call for a change in the legal landscape of electronic privacy.[28] However, in the ever-evolving and fast-

flood of opinions from judges all over the country, see *In re* the Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 433 F. Supp. 2d 804, 804–05 (S.D. Tex. 2006) (listing opinions involving CSLI released in just the first year after Magistrate Judge Orenstein issued his opinion). One of the earliest CSLI opinions indicated in dicta that the gathering of CSLI was not a violation of constitutional rights and fit comfortably within existing law. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) [hereinafter 2005 Texas Opinion] ("[H]istorical cell site data more comfortably fits the category of transactional records covered by the SCA."). Soon thereafter, a district judge in Indiana issued an opinion ruling that historical, as well as prospective, CSLI could not be obtained absent a warrant. *In re* the Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Servs. *in re* the Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info.; and (3) Location of Cell Site Origination &/or Termination, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006) [hereinafter Indiana Opinion] ("The Magistrate Judge described these two requests by stating that one seeks the 'real time' location of the cell phone(s) . . . while the second request seeks 'historical' cell site location information. Either way, the Government is requesting an order requiring cellular phone companies to identify the specific cell tower from which a call originates, is maintained, or received for an incoming or outgoing call. And, as is detailed below, this Court agrees with the Magistrate Judge that such information is unobtainable absent a warrant.").

27. *See generally* W.D. Pa. Opinion, *supra* note 24, at 616; Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009); Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 316 (2004).

28. For example, the Electronic Frontier Foundation has an entire section of its website dedicated to "Cell Tracking." *Cell Tracking*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cell-tracking (last visited Dec. 22, 2011). This portion of the website is replete with links to news articles, press releases, and amicus briefs filed by the Electronic Frontier Foundation in cases dealing with CSLI. *Id.* In addition, recently Senator Patrick Leahy is leading the charge to amend the Electronic Communications Privacy Act so as to provide stronger privacy protections for today's cell phone and Internet users. Declan McCullagh, *Senator Renews Pledge to Update Digital-privacy Law*, CNET (June 16, 2011, 11:39 AM), http://news.cnet.com/8301-31921_3-20071670-281/senator-renews-pledge-to-update-digital-privacy-law/. The new law proposed by Senator Leahy would require the police to obtain a warrant before accessing private electronic communications or real time CSLI. *Id.* It is notable, however, that the subject of this Comment—historical CSLI—would not be affected by Senator Leahy's proposal, because the existing statutory language that has been used to obtain historical CSLI without a showing of probable cause remains untouched. *See id.*

paced world of technology, we should not be so quick to place further restrictions on access to historical CSLI.[29] This Comment aims to clear up some of the current confusion surrounding historical CSLI.

This Comment argues that law enforcement agencies should not be required to obtain a warrant to access records that contain historical CSLI, but rather should be able to gain access to them under the less stringent requirements outlined in the Stored Communications Act (SCA).[30] Moving to a more restrictive standard could have a disastrous effect on the government's ability to guard against threats to public safety.[31] Furthermore, by examining historical CSLI, law enforcement can rarely, if ever, intrude upon any person's reasonable expectation of privacy because the laws and procedures currently in place do not, as some have suggested, pose a threat to our constitutional right to privacy.

Part II of this Comment briefly explains cellular telephone technology and how CSLI is created, as well as differentiates between historical CSLI, which is the subject of this Comment, and real-time CSLI, which is much less controversial in the courts. Part III discusses statutory and case law relevant to the gathering of historical CSLI. Part IV examines the current state of the law, including the recent trend toward a probable cause standard to access historical CSLI, and the recent Third Circuit decision that declines to require such a standard. Part V analyzes the proper standard and argues that the lesser standard enunciated in the SCA is the appropriate standard for historical CSLI. Part VI discusses the impact of moving toward a warrant requirement and some of the harmful consequences that could arise from adopting a probable cause standard for law enforcement to obtain historical CSLI. Part VII concludes.

---

29. Some of the same features that worry privacy advocates make CSLI a "priceless investigative tool" for law enforcement. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1457 (2007). First, whereas tracking devices are often hidden on a suspect's car or other mode of transportation and thus cannot locate a person who uses a different means of conveyance, a cell phone often remains on a suspect's person. *Id.* at 1413. Second, almost all adults in the United States own a cell phone. *Id.* Finally, using CSLI saves money, as there are no expensive devices that must be installed to discover someone's location. *Id.*

30. Under the SCA, the government may obtain records from a cell phone company upon a demonstration of "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . records . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2006).

31. *See infra* notes 303–12 and accompanying text.

II. CELL SITE LOCATION INFORMATION TECHNOLOGY PRIMER

A. Understanding CSLI: Cell Phone Technology

Few people probably spend much time thinking about the infrastructure and technology that makes cell phones work because to use a cell phone, the regular consumer need not know any more than how to dial a phone number.[32] The term "cell phone" is somewhat of a misnomer, as these devices are actually sophisticated radios that transmit sound through frequencies in much the same way that car radios do.[33] Cell phones themselves only have a transmission and receiving range of about three to fifteen miles, so they use a vast and pervasive network of towers to receive and transmit signals between users.[34] Each tower communicates only with the individual cell phones within its transmission range, which is referred to as a "cell."[35] Cells do not have a uniform size or shape due to interference caused by geographical abnormalities such as hills or buildings.[36]

When a cell phone user places a call, a signal is transmitted to the closest cell tower, and then on to the cellular company's mobile telephone

32. In contrast to regular consumers, it is absolutely imperative that attorneys and judges practicing in this area understand how cell phones work and exactly what historical CSLI is before analyzing whether it warrants Fourth Amendment protections. This section aims to provide a concise but complete and relevant description of cell phone technology as of the date of the Comment's publication. Technology evolves so quickly that even Supreme Court Justices occasionally display understandable, yet troubling deficiencies in necessary technological knowledge. Last year, in a case involving violent video games, Justice Kennedy assumed that V-Chips could be utilized by parents to keep kids from playing violent video games. Transcript of Oral Argument at 24–25, Schwarzenegger v. Entm't Merchs. Ass'n, 130 S. Ct. 2398 (2010) (No. 08-1448). As the attorney in the case explained, V-Chips can block *television* programming only. *Id.* Similarly, in another case argued last year, both Chief Justice Roberts and Justice Scalia indicated that they believed text messages pass directly between two phones with no intermediary or third party delivery system. Transcript of Oral Argument at 49, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332). Again, the attorney arguing the case was able to correct this misunderstanding and inform the Court that a text message must first pass through the phone company's computer system before it is sent on to the recipient. *Id.* In both of these cases the attorneys involved were able to correct the Justices and prevent what could have been a misapplication of the law by the highest court in the land. Misconceptions like these could lead well-meaning judges to come to unwarranted conclusions in all sorts of cases related to technology, and the following discussion is meant to help avoid such misunderstandings.

33. Mark Davids et al., *Teaching the Fundamentals of Cell Phones and Wireless Communications*, 48 THE PHYSICS TEACHER 217, 217 (2010).

34. KEN BALDAUF & RALPH M. STAIR, SUCCEEDING WITH TECHNOLOGY: COMPUTER SYSTEM CONCEPTS FOR REAL LIFE 273 (Marie Lee ed., 3d ed. 2009).

35. GUY KLEMENS, THE CELL PHONE: THE HISTORY AND TECHNOLOGY OF THE GADGET THAT CHANGED THE WORLD 54 (2010).

36. *Id.*

switching office.[37] From there, the signal is transferred to the recipient's phone via landlines, other cellular transmission towers, or a combination of the two.[38] Every cell phone has two unique numbers associated with it that are used to facilitate this connection.[39] The first is called a Mobile Identification Number (MIN), which is simply the ten digit number dialed to connect with a particular cell phone user.[40] The second is called an Electronic Serial Number (ESN).[41] This number is unchangeable and is assigned to a particular phone by the mobile communications company that provides service to that phone.[42] Whenever a call is made or received, a record of the call is created and held by the cell phone company, including the individual cell phones involved, those phones' MINs and ESNs, and what cell towers each phone used to transmit the call.[43]

Even when a cell phone is not making or receiving a call, it is still constantly communicating with the broader mobile network.[44] About every seven seconds, a cell phone transmits its MIN and ESN to the nearest cell tower in a process called "registration."[45] While cell phones usually do the transmitting,[46] the process can also work in reverse, and a cell tower can send a signal to a particular phone to determine from where that cell phone is broadcasting its signal.[47] During registration, a cell phone shares its location with a cell tower so that the mobile carrier can quickly and efficiently route calls, and the tower also constantly shares valuable information with the cell phone.[48] The only way to prevent a phone from registering itself is by turning it off.[49] Hence, regardless of whether a cell phone is engaged in a call or simply sitting idle while powered on, it is

37. DEBORAH MORLEY & CHARLES S. PARKER, UNDERSTANDING COMPUTERS: TODAY AND TOMORROW 299 (Marie Lee ed., 12th ed. 2008).

38. *Id.*

39. Recent Development, *supra* note 27, at 309.

40. *Id.*

41. *Id.*

42. *Id.*

43. *See* W.D. Pa. Opinion, *supra* note 24, at 590 & n.20.

44. 2005 Texas Opinion, *supra* note 26, at 751.

45. W.D. Pa. Opinion, *supra* note 24, at 590.

46. Ricky G. Glover, *A Probable Nightmare: Lifting the Fog from the Cellular Surveillance Statutory Catastrophe*, 41 VAL. U. L. REV. 1543, 1549 (2007).

47. *See* New York v. Hall, 823 N.Y.S.2d 334, 338 (Sup. Ct. 2006) (discussing the capacity of T-Mobile, a cell phone company, to "ping" or send a signal to a cell phone that is powered on to determine, in general terms, where that particular phone is).

48. U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 40 (rev. ed. June 2005), *available at* https://www.eff.org/files/filenode/foia_ccips/20080123_esmanual.pdf ("This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.").

49. *See id.*

inevitably (and necessarily) sharing some information about its location with a mobile communications company.

The question naturally follows: exactly how much detail about a cell phone user's location can be discovered by simply analyzing that user's records? Simply knowing which tower is communicating with a particular cell phone is conclusive evidence that a phone is somewhere within that cell tower's broadcasting radius.[50] However, by utilizing more sophisticated measurements taken at the time of transmission, a cell phone's location may be triangulated[51] and determined within 200 feet.[52] The Federal Communications Commission (FCC) even requires that mobile communications companies have the ability to locate ninety-five percent of calls made to or from cell phones accurately within 300 meters or less using methods such as triangulation.[53] If a cell phone is equipped with a GPS device, as almost all phones manufactured today are,[54] the location of that phone could potentially be discerned as accurately as within fifty feet.[55] However, that is a best case scenario, and even with a GPS device, phones

50. *See* Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007). As data is transmitted between cell phones and cell towers, the strength of the signal between the phone and the towers around that phone is measured. *Id.* When a cell phone user changes location, the transmitters recognize that the connection between the phone and its tower is diminishing, but if there is another tower that is receiving a stronger signal, the mobile telephone switching office will recognize this and cause the cell phone to switch frequencies and begin communicating with the new tower. *Id.* So, while a cell phone might transmit its signal to multiple cell towers within its range, it uses only a single cell tower to make or receive calls. *See id.* As discussed above, each cell tower has a transmission range of about three to fifteen miles, so any phone communicating with a given tower must be within that rather large transmission range. *See supra* note 34 and accompanying text.

51. "Triangulation" is a "trigonometric operation for finding a position or location by means of bearings from two fixed points a known distance apart." Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/triangulation?show=0&t=1328408271 (last visited Feb. 7, 2012). Cell towers can be used as fixed points in order to triangulate a position.

52. W.D. Pa. Opinion, *supra* note 24, at 590. One common method of determining location is called Time Distance of Arrival (TDOA), which refers to the process of measuring the time it takes for the signal from a phone to reach a tower. McLaughlin, *supra* note 50, at 426. Companies can also measure the angle between the origin of a signal and a cell phone tower. *Id.* This is called the Angle of Arrival Method (AOA). *Id.*

53. McLaughlin, *supra* note 50, at 426. This requirement is meant to assist 911 operators in locating emergency calls when no location is verbally conveyed. *Id.*

54. *Wireless Issues: Enhanced 911*, VERIZON WIRELESS, http://aboutus.verizonwireless.com/wirelessissues/enhanced911.html (last visited Dec. 22, 2011). Every phone now sold by Verizon Wireless is GPS-enabled in order to comply with FCC mandates. *Id.*

55. McLaughlin, *supra* note 50, at 427. Because of this increased accuracy, when a cell phone is equipped with a GPS device, the FCC mandates that companies be able to locate calls from that device within 150 meters. *Id.*

can generally only be located within a range of 50 to 150 meters.[56] Although some courts have distinguished between information derived from a single tower, from multiple towers, or from GPS technology, any data that can be used to determine a phone's location is collectively referred to as CSLI.[57]

B. Historical CSLI vs. Real Time CSLI

There are two types of CSLI that law enforcement may request from cell phone companies.[58] First, the government can request any records a company has kept containing CSLI.[59] The records obtained under this method are referred to as historical CSLI.[60] Second, they can request to view incoming CSLI as it is received from a user's cell phone in "real time."[61] The information collected through this method is commonly termed prospective CSLI.[62] A majority of courts that have considered applications for real-time CSLI have ruled that the information constitutes tracking information as defined by 18 U.S.C. § 3117, which requires a warrant—and thus a showing of probable cause—before an order for disclosure of that CSLI may be granted.[63]

However, the necessary standard for obtaining historical CSLI is much less certain.[64] When law enforcement agencies request historical CSLI, they can determine the location of a cell phone only at some time in the past.[65] Unlike the real-time CSLI discussed above, this historical CSLI has often been thought to be governed by section 2703 of the SCA, which only requires a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[66] Though this has long been

---

56. *Wireless Issues: Enhanced 911*, *supra* note 54.

57. 2005 Texas Opinion, *supra* note 26, at 754.

58. *See infra* notes 59–62.

59. *See* Deborah F. Buckman, Annotation, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. FED. 2d 537 (2006).

60. *Id.*

61. McLaughlin, *supra* note 50, at 431.

62. Buckman, *supra* note 59.

63. W.D. Pa. Opinion, *supra* note 24, at 595, 601.

64. *See, e.g.*, 2005 Texas Opinion, *supra* note 26, at 748–49 ("The issue explored here has serious implications for the balance between privacy and law enforcement, and is a matter of first impression in this circuit as well as most others.").

65. *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [SEALED] & [SEALED] & the Prod. of Real Time Cell Site Info., 402 F. Supp. 2d 597, 599 (D. Md. 2005).

66. 18 U.S.C. § 2703(d) (2009).

the prevailing interpretation among the courts,[67] some judges have decided that even historical CSLI may only be obtained upon a showing of probable cause.[68] Still others have ruled that no distinction should be made between historical and real-time CSLI, and that CSLI in any form requires probable cause.[69] It is this ambiguity that this Comment is meant to alleviate, so it will focus heavily on the proper standard that should be applied to historical CSLI.

III. LEGAL FRAMEWORK

Due to the nature of modern communications systems such as cell phone networks and the Internet, users of these systems often must entrust personal information to the companies that provide these services.[70] This creates privacy concerns because it is settled law that information voluntarily revealed to a third party is not protected by the Fourth Amendment.[71] The laws and legal principles discussed below were created, in part, to safeguard the privacy of Americans. However, these laws also attempt to provide law enforcement officers with the necessary tools and information to protect the general population. This Comment asserts that the laws below create a workable legal standard that strikes the correct balance between individuals' desire for privacy with the needs of law enforcement.

A. The Fourth Amendment

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

67. *See* McLaughlin, *supra* note 50, at 432 (discussing historical CSLI and concluding that it "would not run afoul of the Court's historical concerns with prospective surveillance").

68. *See, e.g.*, W.D. Pa. Opinion, *supra* note 24, at 595, 600 n.42.

69. *See, e.g.*, Indiana Opinion, *supra* note 26, at *1 (holding that neither of two different requests—one for historical CSLI and one for prospective CSLI—can be granted absent probable cause); *In re* Applications of the United States for Orders Authorizing the Disclosure of Cell Cite [sic] Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005) (ruling that no CSLI requests shall be granted pursuant to 18 U.S.C. § 2703).

70. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004).

71. *See infra* notes 74–76 and accompanying text. *Accord* United States v. Miller, 425 U.S. 435, 443 (1976) (finding no expectation of privacy in information conveyed to third parties "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"); Couch v. United States, 409 U.S. 322 (1973) (holding that there is no reasonable expectation of privacy in documents turned over to an accountant for the purpose of preparing a tax return).

searches and seizures."[72] The purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials."[73] Accordingly, when deciding whether a certain piece of information merits Fourth Amendment protection, a two-pronged test must be satisfied.[74] The first prong requires that an "individual manifested a subjective expectation of privacy in the object of the challenged search."[75] The second prong requires that "society [is] willing to recognize that expectation as reasonable."[76] Therefore, the question of whether the Fourth Amendment protects the location of a certain object or person is dependent upon the individual circumstances of each case.[77]

The Supreme Court has often found occasion to take up questions involving the Fourth Amendment, and these cases provide a lens through which to view the gathering of historical CSLI.[78] For example, in *Smith v. Maryland*, at the request of the police, a telephone company installed a pen register (a device that records the numbers dialed on a telephone) in a suspected robber's home without a warrant or court order.[79] The information from the pen register allowed the police to obtain a search warrant for the suspect's (Smith's) apartment, which led to the discovery of more evidence used against Smith at trial.[80] Smith challenged the warrantless installation of the pen register on his telephone by asserting that he had manifested an expectation of privacy by using the telephone "*in his house* to the exclusion of all others."[81] The Supreme Court ruled that a person holds no reasonable expectation of privacy in the numbers dialed

72. U.S. CONST. amend. IV.

73. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967).

74. California v. Ciraolo, 476 U.S. 207, 211 (1986).

75. *Id.*

76. *Id.*

77. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). *Katz* makes it clear that a piece of information is only protected if someone intends it to be protected. *See id.*

78. While the Supreme Court has never explicitly ruled on the Fourth Amendment challenges to the warrantless gathering of CSLI, see Adam Koppel, Comment, *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, 1080–83 (2010), several cases have dealt with issues essential to the analysis of the proper standard upon which police may obtain historical CSLI. For example, *Smith v. Maryland* dealt with information voluntarily conveyed to a telephone company. Smith v. Maryland, 442 U.S. 735, 744 (1979). *United States v. Knotts* analyzed Fourth Amendment concerns surrounding remote electronic surveillance of persons traveling on public roadways and visible from public places. United States v. Knotts, 460 U.S. 276, 282 (1983). Finally, *United States v. Karo* determined issues surrounding the remote electronic surveillance of person inside a private residence. United States v. Karo, 468 U.S. 705, 717 (1984). Each of these cases and the holdings are discussed in greater detail below. *See infra* notes 79–98.

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

80. *Id.*

81. *Id.* at 743.

from a home telephone, and thus the collection of such evidence by the government does not constitute a search under the Fourth Amendment.[82] The Court further stated that even though Smith was in his own home, the location where a call is placed should not be considered in determining whether the caller retains any expectation of privacy in the dialed numbers.[83]

The Court later decided two cases, *United States v. Knotts*[84] and *United States v. Karo*,[85] that both may aide in determining when a person possesses a reasonable expectation of privacy as to his or her location.[86] These cases are especially apt when discussing historical CSLI because they dealt with a technology that many critics of the current interpretation of the SCA compare to cell phones: tracking devices.[87]

In *Knotts*, police officers became suspicious that a man named Armstrong was purchasing chloroform to produce illicit drugs.[88] With the consent of the company selling the chloroform, police placed a beeper (a type of tracking device) inside barrels containing Armstrong's next purchase.[89] After Armstrong picked up the chloroform, police used both visual surveillance and the beeper's signal to discover Armstrong's presence at a cabin in Wisconsin that contained a makeshift drug laboratory.[90] In a unanimous decision, the Supreme Court ruled that the police did not violate the Fourth Amendment by monitoring the beeper's signal to locate the suspect because during the entire time he was being monitored, the suspect was either traveling on public roads or was clearly visible from the vantage

82. *Id.* (citing Brief for Petitioner at 6, Smith v. Maryland, 442 U.S. 735 (1979) (No. 78-5374)). The Supreme Court stated that because the information (dialed numbers) had been "voluntarily conveyed" to the phone company, Smith had "assumed the risk" that the phone company would disclose the same information to the police. *Id.* at 745. Thus, because of this risk, Smith could have no reasonable expectation that the numbers he had dialed would remain private. *Id.* This analysis remained true, the Court said, even though the telephone system was completely automated, and no human operator had connected the calls. *Id.*

83. *Id.* Smith argued that because he used the telephone in his private residence, he "demonstrated an expectation of privacy by his own conduct." *Id.* at 743. The Court speculated that his "conduct may have been calculated to keep the *contents* of his conversation private," but this was immaterial to an analysis of whether a dialed number may be obtained, because, regardless of a person's location, that person must "convey that number to the telephone company in precisely the same way if he wished to complete his call." *Id.*

84. 460 U.S. 276 (1983).

85. 468 U.S. 705 (1984).

86. *See infra* notes 88–98.

87. *See infra* notes 88–98.

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

89. *Id.*

90. *Id*. at 278–79.

point of a public place.[91] In arriving at this conclusion, the Court reasoned that the circumstances under which the beeper was used provided roughly the same information to the police that a patrol car following the suspect could have.[92] In other words, the suspect had no reasonable expectation of privacy in the location of the chloroform while it was traveling in a truck on the public roadways, or while it was clearly visible outside the suspect's private residence.[93]

In *Karo*, police planted a beeper (the same type of tracking device used in *Knotts*) in a can of ether purchased for the purpose of extracting cocaine from clothing smuggled into the country.[94] Using both visual surveillance and the beeper's signal, the police followed the can of ether to the house of one of the defendants in the case.[95] The cans of ether were moved three

---

91. *Id.* at 281–82, 285. Although this was a unanimous decision, three concurring opinions were filed, indicating differences of opinion in the reasoning that should be used to arrive at the result. *See id.* at 285–88. Also, the issue in this case was notably confined only to whether the *monitoring* of the beeper was constitutional. *Id.* at 279. Justice Brennan, in his concurring opinion, indicated that this "would have been a much more difficult case if respondent had challenged, not merely certain aspects of the monitoring of the beeper installed in the chloroform container purchased by respondent's compatriot, but also its original installation." *Id.* at 286 (Brennan, J., concurring). However, for the purposes of this Comment, the issue of installation is irrelevant, as obtaining historical CSLI requires no special equipment and does not even require any physical proximity to a particular cell phone. *See In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 81 n.11 (D. Mass. 2007) ("The 'tracking' of a cell phone does not require the installation of any sort of device.").

92. *See Knotts*, 460 U.S. at 282 ("The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

93. *See id.* The Court indicated that the "open fields" doctrine applied. *Id.* Simply put, this doctrine dictates that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields." Hester v. United States, 265 U.S. 57, 59 (1924). As it is used here, the term "open fields" simply refers to "any unoccupied or undeveloped area outside of the curtilage" of a home. Oliver v. United States, 466 U.S. 170, 180 n.11 (1984). Thus, "[a]n open field need be neither 'open' nor a 'field' as those terms are used in common speech." *Id.* Justice Blackmun challenged the applicability of this doctrine to the *Knotts* case. *Knotts*, 460 U.S. at 287 (Blackmun, J., concurring) ("For me, the present case does not concern the open fields doctrine, and I regard these references and citations as unnecessary for the Court's decision."). Regardless of whether the open fields doctrine applies to this particular case, it does provide one important insight into Fourth Amendment jurisprudence: constitutional protections will not attach to an object simply because it is on private rather than public property. *See id.* at 285 (majority opinion) ("[N]otions of physical trespass based on the law of real property were not dispositive in *Katz* . . . ."); *Oliver*, 466 U.S. at 180 ("[C]ourts have extended Fourth Amendment protection to the curtilage; and they have defined the curtilage, as did the common law, by reference to the factors that determine whether an individual reasonably may expect that an area immediately adjacent to the home will remain private. Conversely, the common law implies, as we reaffirm today, that no expectation of privacy legitimately attaches to open fields." (internal citations omitted)).

94. United States v. Karo, 468 U.S. 705, 708 (1984).

95. *Id.* at 708–10.

times to three different houses completely undetected by the visual surveillance of any police officers, but were located *after* each move had been completed by the sole use and monitoring of the beeper.[96] This case differed from *Knotts* in that the police used the beeper to determine the location of the bugged barrel of ether while it was inside a private residence and removed entirely from public view, not while it was in a public place or visible to public view.[97] This distinction caused the Supreme Court to rule that this warrantless use of a tracking device *was* a violation of the Fourth Amendment.[98]

The critical difference between *Knotts* and *Karo* was not *how* the location information was ascertained, but rather *where* the beepers were while broadcasting their location to the police.[99] The Court recognized in *Karo* that electronic devices such as beepers could be used to discover facts that "the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[100] Thus, a critical question to consider when analyzing electronic surveillance cases is what kind of information can be collected and whether that sort of information would be

---

96. *Id.*

97. *Id.* at 714.

98. *See id.* at 718. The following passage from *Karo* has particular significance to this Comment, as it is perhaps the largest hurdle to overcome in arguing that the warrantless gathering of historical CSLI is not a violation of the Fourth Amendment:

> We cannot accept the Government's contention that it should be completely free from the constraints of the *Fourth Amendment* to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of *Fourth Amendment* oversight.

Id. at 716 (emphasis added). This Comment argues that a warrant should not be required to access historical CSLI, which seems to be the type of indiscriminate monitoring that *Karo* was concerned about. This does not end the matter, however, because in her concurring opinion, Justice O'Connor tempered the strong and definitive tone of this assertion when she said:

> As a threshold matter it is clear that the mere presence of electronic equipment inside a home, transmitting information to government agents outside, does not, in and of itself, infringe on legitimate expectations of privacy of all who have an expectation of privacy in the home itself. . . . We must therefore look for something more before concluding that monitoring of a beeper in a closed container that is brought into a home violates the homeowner's reasonable expectations of privacy.

Id. at 722–23 (O'Connor, J., concurring in part and concurring in the judgment). Similarly, courts should look for "something more" before concluding that *all* warrantless gathering of historical CSLI constitutes a violation of the Fourth Amendment.

99. *See id.* at 715 (majority opinion).

100. *Id.*

freely available to, say, a passerby.[101] The fact that the information is gathered surreptitiously by electronic surveillance might make it *seem* improper, but, the Supreme Court spoke very clearly to the legality of such surveillance techniques when it said, "[n]othing in the *Fourth Amendment* prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[102] Due in part to advances in technology, Congress has occasionally stepped in with legislation aimed at providing Americans with protections beyond those provided by the Constitution.

B. The Stored Communications Act

The SCA[103] was passed in 1986 as part of the Electronic Communications Privacy Act of 1986.[104] In response to privacy concerns surrounding the advancement of communications technology, Congress enacted the SCA to provide some statutory protection of personal information where traditional Fourth Amendment protections were lacking.[105] The SCA does two important things to protect information. First, it limits the government's ability to compel private communications companies to disclose information about subscribers.[106] Second, it limits a

---

101. For example, *Knotts* focused on what it was the police learned by monitoring the beeper and came to the following conclusion:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

United States v. Knotts, 460 U.S. 276, 281–82 (1983). Note that the Court is focused on the traveler's actions, and not the police's actions. *See id.* Presumably, had the same information been gathered from the traveler's cell phone rather than a beeper, the Court would have come to the same conclusion.

102. *Id.* at 282 (emphasis added). A similar sentiment appears in *Smith v. Maryland*, in which the petitioner argued that because his phone call was connected through an automated service rather than a live operator, the number he dialed was not voluntarily shared by him and thus deserved constitutional protection. *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1979). The Court dismissed this argument, stating "[w]e are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." *Id.*

103. 18 U.S.C. §§ 2701–2710 (2006).

104. The SCA is contained in Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

105. Kerr, *supra* note 70, at 1212.

106. 18 U.S.C. § 2703 (2006) (detailing the evidentiary standard that must be met to obtain certain types of information from companies). Prior to the passing of the SCA, the government likely could have obtained personal subscriber information (such as e-mails) from companies simply by issuing a subpoena. *See* Kerr, *supra* note 70, at 1213. Though the protections provided by the SCA are not always as strong as those provided by the Fourth Amendment, it does provide greater protection than consumers had prior to its passing. *Id.*

private company's ability to voluntarily turn over information about a subscriber to the government.[107]

The SCA is a relatively narrow statute, and it only protects information held by two specific types of service providers.[108] The first type of provider is an electronic communication service (ECS), which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[109] The second provider is a remote computing service (RCS), which refers to "computer storage or processing services by means of an electronic communications system."[110] The distinction between an ECS and an RCS at times seems confusing or even arbitrary, but for the purpose of this Comment, a lengthy discussion of differentiating characteristics is unnecessary.[111] This is because a single provision of the SCA, 18 U.S.C. § 2703(c), grants the authority and outlines the procedures by which government officials may require historical CSLI to be disclosed by providers of *either* an ECS or an RCS.[112] For the sake of clarity, however, even though cell phone companies may act as both an ECS and an

107. Kerr, *supra* note 70, at 1213. The SCA contains a general prohibition against private companies disclosing records of their subscribers to governments, but then provides exceptions under which disclosure is proper. *See* 18 U.S.C. § 2702 (2006).

108. Kerr, *supra* note 70.

109. 18 U.S.C. § 2510(15) (2006).

110. *Id.* § 2711(2). An electronic communications system (not to be confused with an electronic communication service) is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

111. Kerr, *supra* note 70, at 1215–16 ("The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract. A provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications. In the case of a public provider, for example, files held in intermediate 'electronic storage' are protected under the ECS rules; meanwhile, files held for long-term storage by that same provider are protected by the RCS rules.").

112. 18 U.S.C. § 2703 (2006). The authority to compel disclosure granted by this section of the SCA is limited and specifically excludes the contents of any communications—such as a voice recording of a phone call or the text of an e-mail. *Id.*

RCS,[113] they are almost certainly acting as providers of ECS when they gather historical CSLI.[114]

The SCA provides a number of avenues through which the government can seek records from an ECS or an RCS.[115] The two options most relevant to this Comment are to obtain a warrant or to obtain a court order pursuant to 18 U.S.C. § 2703(d).[116] In stark contrast with the standard necessary to obtain a warrant (probable cause),[117] section 2703(d) only requires law enforcement to offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[118] Because these two options are presented in the SCA, courts have often suggested it is permissible for law enforcement officials seeking historical CSLI to choose the less stringent of these standards and obtain court orders by satisfying only the "specific and articulable facts" standard outlined in 18 U.S.C. § 2703(d).[119] While these sections of the SCA focus on when law enforcement can request information from companies, the legislation discussed in the next sections helps ensure that companies are retaining the type of information law enforcement might find useful.

---

113. Kerr, *supra* note 70, at 1215 ("[M]ost network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in other contexts, and as neither in some contexts as well. . . . The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract.").

114. *See In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) ("Cell phone service providers clearly fit within [the definition of an ECS].").

115. 18 U.S.C. § 2703(c) (2006). According to the law, the government may require disclosure from an ECS or RCS when they (1) obtain a warrant, (2) obtain a court order, (3) obtain consent from a customer or subscriber, or (4) use a formal written request for basic contact information for a customer or subscriber suspected of telemarketing fraud. *Id.* § 2703(c)(1)(A)–(D).

116. *Id.* § 2703(c)(1)(A)–(B). Cell phone records, including historical CSLI, may also be obtained by the government if the government has the consent of the subscriber or in special cases dealing with telemarketing fraud. *Id.* § 2703(c)(1)(C)–(D).

117. U.S. CONST. amend. IV.

118. 18 U.S.C. § 2703(d) (2006).

119. *See, e.g.*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) ("Because historical cell site information clearly satisfies each of the three definitional requirements of section 2703(c), a section 2703(d) order requiring the disclosure of historical cell site information may issue on a showing of 'specific and articulable facts' and no more."); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 303 n.6 (E.D.N.Y. 2005) (asserting in dicta that 18 U.S.C. § 2703(d) "plainly allows" the government to request historical CSLI); 2005 Texas Opinion, *supra* note 26, at 759 n.16 ("[H]istorical cell site data more comfortably fits the category of transactional records covered by the SCA. Cell phone companies might legitimately compile such data for customized marketing and billing purposes.").

C. The Communications for Assistance of Law Enforcement Act

The Communications for Assistance of Law Enforcement Act (CALEA) was passed in 1994.[120] Simply, CALEA defines the scope and limits of the duty of companies to cooperate with the government in intercepting communications.[121] CALEA requires communications service providers to implement their services in a way that will allow the government to later intercept or otherwise access "all wire and electronic communications carried by the carrier within a service area to or from equipment."[122] To access particular wire or electronic communications, law enforcement officials must have the proper authority—such as a warrant or a court order—and communications providers are tasked with the responsibility of making their systems secure from unauthorized access by law enforcement.[123] Likely in response to concerns over the government's power to misuse information received from communications companies,[124] the CALEA expressly forbids companies from turning over "call-identifying information" in such a way as to indicate the physical location of a subscriber.[125] However, this only applies when the government is acting "solely pursuant to the authority for pen registers and trap and trace devices."[126] Legislation governing these devices is discussed next.

D. The Pen Register Statute

The Pen Register Statute[127] was passed in 1986 and, along with the SCA, forms part of the Electronic Communications Privacy Act.[128] A pen

120. Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C.A. §§ 1001 to 1010*, 25 A.L.R. FED. 2d 323, 323 (2008).

121. *Id.* at 333.

122. 47 U.S.C. § 1002(a)(1)–(4) (2006).

123. *See id.* § 1004 ("A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer . . . acting in accordance with regulations . . . .").

124. *See* W.D. Pa. Opinion, *supra* note 24, at 596–98 (recounting testimony given to Congress addressing the concern that "law enforcement could obtain—by CSLI—information of an individual's physical movement previously obtainable only through visual surveillance or the covert installation of a radio-wave transmitter").

125. 47 U.S.C. § 1002 (2006).

126. *Id.*

127. 18 U.S.C. §§ 3121–3127 (2006).

128. Buckman, *supra* note 59.

register is "a mechanical device that logs dialed telephone numbers" without recording the content of the conversation.[129] While pen registers monitor the phone numbers dialed for outgoing calls, trap and trace devices identify the phone numbers of incoming calls.[130] The Pen Register Act outlines the conditions under which the government may use a pen register or trap and trace device.[131] When this law was originally passed, the definitions of a pen register and a trap and trace device were relatively narrow, applying only to devices used on telephones.[132] However, that definition was significantly broadened in 2001 with the passage of the USA PATRIOT Act[133] to include in its application not only telephones, but information from any "wire or electronic communication."[134]

Because of the Supreme Court's ruling in *Smith v. Maryland*[135] that numbers dialed on a telephone do not warrant Fourth Amendment protection,[136] the standard of proof that law enforcement officials must meet in order to install a pen register or trap and trace device is quite low.[137] To install either of these devices, government officials only need to show that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[138]

---

129. BLACK'S LAW DICTIONARY 1248 (9th ed. 2009).

130. Buckman, *supra* note 59.

131. *See* 18 U.S.C. § 3121 (2006).

132. 18 U.S.C. § 3127 (2000) (amended 2001). In the original version of the Pen Register Statute, a "pen register" was defined as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." *Id.* A "trap and trace device" was defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." *Id.* § 3127(4).

133. *See* Buckman, *supra* note 59. Today, a pen register is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," and a trap and trace device is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(3)–(4) (2006).

134. 18 U.S.C. § 3127 (2006). The USA PATRIOT Act's amendment gave the Pen Register Statute a violent shove into the twenty-first century, and, in so doing, ensured that the government could utilize pen registers and trap and trace devices not only on telephones, but also on cell phones and even personal computers. Susan W. Dean, Comment, *Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law Under the Patriot Act*, 5 TUL. J. TECH. & INTELL. PROP. 97, 101 (2003).

135. 442 U.S. 735 (1979).

136. *See supra* note 82 and accompanying text.

137. Buckman, *supra* note 59.

138. 18 U.S.C. § 3123(a)(1) (2006).

IV. THE PUSH FOR A PROBABLE CAUSE STANDARD

Courts began publishing opinions regarding issues surrounding CSLI in 2005.[139] While courts are still divided as to whether real-time CSLI may be obtained by a showing of less than probable cause,[140] there have been relatively few cases that have taken up the issues surrounding purely historical CSLI.[141] Over the last several years, the prevailing view among the courts was that historical CSLI was governed by the SCA and thus could be obtained without a warrant pursuant to an 18 U.S.C. § 2703(d) order.[142] Furthermore, the use of historical CSLI in criminal investigations is a common practice among law enforcement agencies all over the country.[143]

In 2008, Magistrate Judge Lisa Pupo Lenihan of the Western District of Pennsylvania wrote a lengthy denial of an application to compel a cell phone service provider to disclose historical CSLI.[144] In her opinion, Judge Lenihan concluded in unequivocal terms that "mandating a cell phone service provider's covert disclosure of individual subscribers' . . . physical location information must be accompanied by a showing of probable

139. *See supra* note 26.

140. *See* Koppel, *supra* note 78, at 1080–83 (citing, among others, *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 460–61 (S.D.N.Y. 2006) (requiring less than probable cause); *In re* an Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (requiring probable cause)).

141. W.D. Pa. Opinion, *supra* note 24, at 599–600.

142. *See, e.g.*, 2005 Texas Opinion, *supra* note 26, at 748–49. It is difficult if not impossible to know exactly how often requests for historical CSLI are granted, because the opinions granting or denying these requests are often sealed. *Id.* at 748. However, the court here described the government's choice to combine a request for historical CSLI records with a request for a pen register and trap and trace device as "standard practice." *Id.* at 749. Furthermore, in this case, the court had already granted the government's request for historical CSLI without issuing a public opinion. *Id.* at 748.

143. Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Affirmance of the District Court at 15, *In re* the Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585 (2008) (No. 08-4227) ("FBI Special Agent and CSLI expert William Shute testified that he has used historical cell site information to locate fugitives almost 150 times."). *See, e.g.*, Christian Nolan, *Can Your Cell Phone Put You in a Cell Block?*, LAW TECHNOLOGY NEWS (July 7, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202463302148 (stating that federal officials, while investigating four bank robberies, "obtained the [historical CSLI] and phone records of 169 cell phone numbers from nine separate providers").

144. W.D. Pa. Opinion, *supra* note 24.

cause."[145] The court reasoned that the technology used to gather CSLI has essentially made cell phones indistinguishable from tracking devices.[146]

This case is particularly noteworthy because, in an exceedingly rare show of solidarity, all four of the other magistrate judges in the Western District of Pennsylvania joined in the opinion.[147] Though the court's opinion was reversed on appeal,[148] it represents a growing consensus among judges that historical CSLI deserves Fourth Amendment protection.[149]

After Judge Lenihan issued her opinion in 2008, the Third Circuit took up the appeal and became the first federal appeals court to consider whether a warrant is required for the government to order disclosure of historical CSLI.[150] The Third Circuit quickly dismissed the district court's contention that cell phones are tracking devices by pointing out that the historical CSLI records sought were actually derived from a wire communication and not an electronic communication.[151] This is significant because while tracking devices are excluded from the definition of electronic communications, they

---

145. *Id.* at 586.

146. *Id.* at 602 ("[O]ur cell phones, whenever on, broadcast this information virtually continuously as we go about from place to place. Even without triangulation, our cell phones transmit . . . information of our movements to a few hundred feet. It is, therefore, extremely difficult to see how a cell phone is not now *precisely* an 'electronic . . . device which permits the tracking of the movement of a person or object.'" (quoting 18 U.S.C. § 3119(b) (2006)).

147. *See id.* at 616. On appeal, the Third Circuit noted:

> [T]he [Magistrate Judge's] opinion was joined by the other magistrate judges in that district. This is unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues who, after all, routinely issue warrants authorizing searches and production of documents.

In re the Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308 (3d Cir. 2010) [hereinafter Third Circuit Opinion].

148. Third Circuit Opinion, *supra* note 147, at 319.

149. This growing consensus is evidenced by the fact that even while the Third Circuit was considering its appeal, Magistrate Judge Lenihan's opinion was cited with approval by a court in Texas. *In re* the Application of the United States for an Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Information; & (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 584 n.21 (W.D. Tex. 2010) [hereinafter 2010 Texas Opinion].

150. Third Circuit Opinion, *supra* note 147, at 306.

151. *Id.* at 310. A wire communication is defined as: "[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 (*including the use of such connection in a switching station*)." 18 U.S.C. § 2510(1) (2006) (emphasis added). A cell tower collected the information sought in this case (and likely numerous other historical CSLI requests) only when a call was made. Third Circuit Opinion, *supra* note 147, at 310. Cell towers are essentially switching stations for phone calls, and thus the historical CSLI in this case fit squarely within the definition of a wire transfer. *See supra* note 37 and accompanying text. *See also infra* notes 189–221 and accompanying text for a more detailed analysis of this issue.

are *not* excluded from the definition of wire communications.[152] By correctly classifying cell phone calls as wire communications, the court ruled that whether a cell phone is a tracking device was "irrelevant" to this case because the SCA does not prohibit the gathering of CSLI from tracking devices, as long as the tracking devices are wire communications.[153]

The Third Circuit did not reject the argument that cell phones may at times resemble tracking devices.[154] However, it did reject the notion that "CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production."[155] Accordingly, the court strongly and definitively stated that "CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order *does not require the traditional probable cause determination*."[156] However, the fact remains that the SCA provides two paths to obtaining historical CSLI: (1) a § 2703(d) order, and, (2) a warrant.[157] The Third Circuit was "stymied" by the lack of any clear indication by Congress in the text of the SCA for when law enforcement should obtain a § 2703(d) order and when they must obtain a warrant.[158] The court did little to alleviate this uncertainty and ruled that it was within a trial court's discretion whether or not to require a warrant when applications for historical CSLI are presented to them, but that the option to require a warrant should be used "sparingly."[159]

Because it was the first circuit court to address the issue of historical CSLI, the Third Circuit's decision will likely guide future courts in analyzing this important issue.[160] The next section will focus on a question that the Third Circuit left to the discretion of the trial court judge: When does an order to compel the disclosure of historical CSLI deserve the protection of the Fourth Amendment?[161]

---

152. 18 U.S.C. § 2510(1), (12) (2006). A more comprehensive analysis of this issue appears below. *See infra* notes 191–215.

153. *See* Third Circuit Opinion, *supra* note 147, at 310.

154. *Id.* at 312.

155. *Id.* at 313.

156. *Id.* (emphasis added).

157. *Id.* at 319.

158. *Id.*

159. *See id.* ("Because the statute as presently written gives the MJ the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly because Congress also included the option of a § 2703(d) order.").

160. *See id.* at 305–06. The court stated in its opinion that the appeal was its "first opportunity to review whether a court can deny a Government application under 18 U.S.C. § 2703(d) after the Government has satisfied its burden of proof under that provision, a task that to our knowledge *has not been performed by any other court of appeals*." *Id.* (emphasis added).

161. *See infra* Part V.

V. WHY COURTS SHOULD REJECT A WARRANT REQUIREMENT FOR HISTORICAL CSLI

A. The SCA Applies to Historical CSLI

1. A Cell Phone Is Not a Tracking Device

A common argument used by privacy advocates is that the gathering of CSLI has the ability to turn a cell phone into a de facto tracking device.[162] Terminology matters here because if a cell phone *is* a tracking device, the government may not be able to use the SCA at all to compel disclosure of historical CSLI.[163] This is because the SCA specifically excludes tracking devices from its definition of an "electronic communication."[164] Thus, to obtain historical CSLI, the information must have been stored by an ECS (a company that provides electronic communications).[165] This has led some to argue that historical CSLI—because it originates from what they call a de facto tracking device—falls outside the SCA's authority.[166] If this is correct, and cell phones are tracking devices *and* transmit electronic communications, there is no other statutory avenue through which the government could compel the disclosure of CSLI, leaving law enforcement with no other option but to seek a warrant.[167] The debate over whether modern cell phones are tracking devices is more than just a rhetorical one; in fact, if true it has serious implications for law enforcement on the ground and the admissibility of evidence in court.

Some legal precedent suggests that prospective (real time) CSLI is considered information from a tracking device,[168] but this is another question for another article. In this Comment, the concern is the proper interpretation of *historical* CSLI. Because historical CSLI can only communicate a person's location at some point in the past, it is less of a threat to privacy and

---

162. *See, e.g.*, Peter J. Sampson, *Cellphones Give Feds Insight into Criminal Activity*, NORTHJERSEY.COM, Jan. 17, 2011, http://www.northjersey.com/news/114072489_Feds_dialed_in_to_criminals.html?c=y&page=2 ("People should be concerned because, whether they realize it or not, they're carrying a tracking device in their pocket.").

163. *See infra* note 167 and accompanying text.

164. 18 U.S.C. § 2510(12)(C) (2006).

165. *Id.* § 2703(c). Records from an RCS can also be obtained under this statute. *Id.*

166. *See, e.g.*, *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, & for Geographic Location Info., 497 F. Supp. 2d 301, 310–11 (D.P.R. 2007).

167. Chamberlain, *supra* note 27, at 1776 ("Because historical CSLI falls squarely within the tracking device definition . . . it necessarily falls outside the scope of the SCA.").

168. *See, e.g.*, 2005 Texas Opinion, *supra* note 26, at 751 ("While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data.").

thus less deserving of Fourth Amendment protections.[169] An in-depth analysis of the SCA demonstrates the veracity of this statement and refutes the contention that historical CSLI should be considered information from a tracking device at all.[170]

For the purpose of the SCA, a tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[171] At first glance, case law would seem to support the interpretation that historical CSLI is information obtained from a tracking device.[172] However, it would be unfair to classify this as the prevailing interpretation among courts throughout the country.[173] The current debate is nicely illustrated by a 2008 case in which a federal magistrate judge in Pennsylvania ruled that a warrant was required for the government to compel the disclosure of historical CSLI, and in doing so relied heavily on her determination that historical CSLI constituted information from a tracking device.[174] On appeal, the Third Circuit admitted that cell phones "resemble" tracking devices, but nonetheless explicitly rejected the lower court's conclusion that historical CSLI was, by definition, information from a tracking device.[175]

---

169. *See* Koppel, *supra* note 78, at 1068–69 (discussing historical CSLI's "limited" value and the fact that it produces a "lower level of concern from privacy advocates").

170. *See infra* notes 174–90.

171. 18 U.S.C. § 3117(b) (2006).

172. One of the first district courts to issue an order denying a request for CSLI found that not only are cell phones easily converted into tracking devices when CSLI is monitored in real time, but also noted that cell phones and modern tracking devices actually share much of the same technology. 2005 Texas Opinion, *supra* note 26, at 753–56. This decision has been heavily relied on by courts denying requests for historical CSLI on similar grounds. *See, e.g.*, W.D. Pa. Opinion, *supra* note 24, at 600 n.41.

173. At least one court found no distinction between historical CSLI and any other form of business record. United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008). Others have simply found that historical CSLI does not meet the definition of a tracking device. *E.g.*, *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 449 n.8 (S.D.N.Y. 2005).

174. W.D. Pa. Opinion, *supra* note 24, at 616.

175. Third Circuit Opinion, *supra* note 147, at 312–13. The Third Circuit did not take a strong stance on whether or not cell phones were tracking devices, but rather looked beyond that point to focus on the privacy issues at play:

> We cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject. The *Knotts*/*Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home. 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. We therefore cannot

18 U.S.C. § 2703(c), the critical statute allowing for historical CSLI requests, borrows its definition of a tracking device from 18 U.S.C. § 2510(12)(C).[176] However, 18 U.S.C. § 2510 in turn incorporates the definition of tracking devices "as defined in section 3117 of this title."[177] Thus, courts defining cell phones as tracking devices often rely on the seemingly unambiguous definition of tracking devices found in subsection (b) of 18 U.S.C. § 3117: "an electronic or mechanical device which permits the tracking of the movement of a person or object."[178] This definition, while simple and straightforward, is incomplete.

Relying solely on subsection (b) and ignoring subsection (a) of 18 U.S.C. § 3117 for the definition of a tracking device is incorrect because according to well-accepted principles of statutory construction, "[n]o clause, sentence or word shall be construed as superfluous, void or insignificant if a construction can be found which will give force to and preserve all the words of the statute."[179] This means that 18 U.S.C. § 3117 must be read and interpreted as a whole by incorporating subsections (a) and (b) *both* into the definition of a tracking device.[180]

18 U.S.C. § 3117(a) states: "If a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."[181] This subsection of the statute refers only to the "installation" of a tracking device by the government.[182] When a request for historical CSLI for a particular phone is made, nothing is installed, nor has anything ever been installed on that phone by the government.[183] In accordance with this line of reasoning, several courts have ruled that the SCA's definition of a tracking device

---

> accept the MJ's conclusion that CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production.

Id.

176. 18 U.S.C. § 2510 (2006) defines several terms used in the chapter containing the SCA.

177. *Id.* § 2510(12)(C).

178. *Id.* § 3117(b); *see In re* Applications of United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. & Historical Cell Site Info. for Mobile Identification Numbers: (XXX) XXX-AAAA, (XXX) XXX-BBBB, & (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 76 (D. Mass. 2007) [hereinafter Massachusetts Opinion] ("[H]istoric cell site information effectively acts as a 'real time' tracking device, as contemplated by the broad definition of 18 U.S.C. § 3117(b)."), *rev'd sub nom*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

179. NORMAN J. SINGER & J.D. SHAMBIE SINGER, STATUTES AND STATUTORY CONSTRUCTION § 46:6 (7th ed. 2007).

180. *See id.*

181. 18 U.S.C. § 3117(a) (2006) (emphasis added).

182. *Id.*

183. *See supra* note 43 and accompanying text. CSLI simply consists of electronic records of routine communications between a cell phone and the larger mobile network. *See supra* note 43 and accompanying text.

simply does not, and cannot, apply to cell phones.[184] This leads to the conclusion that for the purposes of the SCA, cell phones can never be considered tracking devices.[185]

Most courts have thus far declined to adopt the definition of a "tracking device" elucidated above, but have instead ruled that the language in 18 U.S.C. § 3117(b) alone defines tracking devices under the SCA.[186] Admittedly, when a court restricts itself in this way, it is difficult to avoid the conclusion that "the definition [of a tracking device] is striking for its breadth."[187] However, the crucial language in 18 U.S.C. § 3117(a) indicates that 18 U.S.C. § 3117 as a whole can only govern devices that must be installed, meaning that cell phones necessarily fall well outside that definition.[188]

2. A Cell Phone Is a Wire Communication

Although the tracking device question analyzed above has been a major feature in many cases involving CSLI,[189] it could be inconsequential when

184. *See In re* Applications of United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 81 n.11 (D. Mass. 2007) ("The statute governs the 'installation' of tracking devices. The 'tracking' of a cell phone does not require the installation of any sort of device. The telephone does the job by itself."); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) ("Section 3117 speaks only to the 'installation' of a tracking device. Here, the government does not seek to *install* any sort of tracking device, as cell phones provide location information on their own by transmitting signals to nearby antenna towers.").

185. Though courts have been making this argument since as early as 2006, *supra* note 143, some commentators arguing historical CSLI deserves Fourth Amendment protections have neglected to give this statutory construction argument any treatment whatsoever. *E.g.*, Chamberlain, *supra* note 27; Koppel, *supra* note 78. For example, in his 2009 article, Mr. Chamberlain ignores this argument, which is necessarily intertwined with legislative intent, and then later paradoxically calls for legislative action. Chamberlain, *supra* note 27, at 1788–89. Before asking Congress to speak again, it is prudent to fully explore what Congress has already said on the issue.

186. Massachusetts Opinion, *supra* note 178, at 74 (citing several district courts that have relied on section 3117(b) to adopt a broad definition of tracking devices), *rev'd sub nom*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76.

187. 2005 Texas Opinion, *supra* note 26, at 753.

188. *See* 18 U.S.C. § 3117(a) (2006).

189. *See, e.g.*, 2010 Texas Opinion, *supra* note 149, at 578–80 (finding both prospective and historical CSLI are information from a tracking device); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 460 (S.D.N.Y. 2006) (finding historical CSLI is not information from a tracking device); Massachusetts Opinion, *supra* note 178, at 74, *rev'd sub nom.*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d at 69 (D. Mass. 2007) (finding historical CSLI is information from a tracking device); *In re* the Application of the United States for

determining whether or not the government can use the SCA to obtain historical CSLI.[190] The Third Circuit, though it seemed to accept the possibility that CSLI could be considered information from a tracking device,[191] explicitly stated that the tracking device question was "irrelevant" for the purposes of its analysis.[192] The court instead ruled that the prohibition against requesting tracking device information does not apply to cell phones because cell phones—according to the relevant statutory definition—are "wire communications."[193]

The portion of the SCA that the government relies on to compel cell phone companies to turn over historical CSLI applies only to ECSs and RCSs.[194] As discussed in Part II.B. above, when gathering historical CSLI, cell phone companies are acting as ECSs.[195] An ECS is defined in the SCA as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[196] Of course, the definitions for wire and electronic communications differ under the SCA,[197] and they vary in one extremely important way: while the definition of an electronic communication specifically excludes tracking devices, the definition of a wire communications does not.[198]

Courts that have rejected orders to compel disclosure of historical CSLI based on the determination that cell phones are tracking devices assume that cell phone transmissions constitute electronic communications.[199] However,

---

an Order Authorizing the Installation of a Pen Register Device, a Trap & Trace Device, & for Geographic Location Info., 497 F. Supp. 2d 301, 310–11 (D.P.R. 2007) (finding prospective CSLI is information from a tracking device); *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 449–50 (S.D.N.Y. 2005) (holding that historical CSLI is not information from a tracking device).

190. *See infra* notes 191–221.

191. *See supra* note 139 and accompanying text.

192. Third Circuit Opinion, *supra* note 147, at 310 ("[E]ven if the record of a cell phone call does indicate generally where a cell phone was used when a call was made, so that the resulting CSLI was information from a tracking device, that is irrelevant here because the CSLI derives from a 'wire communication' and not an 'electronic communication.'"). To be clear, the Third Circuit stated the tracking device question was irrelevant only to its statutory interpretation analysis. *Id.* The court still performed a full Fourth Amendment analysis on the historical CSLI requested in the case and found no constitutional violations. *Id.* at 311–12.

193. *Id.* at 310. This is due to the fact that cell phone transmissions qualify as wire communications, and tracking devices are not excluded from wire communications. *See* 18 U.S.C. § 2510(1) (2006).

194. 18 U.S.C. § 2703(d) (2006).

195. *See supra* note 114 and accompanying text.

196. 18 U.S.C. § 2510(15) (2006).

197. *Compare id.* § 2510(1), *with id.* § 2510(12).

198. *Id.* § 2510(1), (12).

199. *See* W.D. Pa. Opinion, *supra* note 24, at 616 (concluding that because historical CSLI is a tracking device it does not fit the definition of an electronic communication and falls outside the reach of the SCA). *See also* 2010 Texas Opinion, *supra* note 149, at 575 n.10 ("[T]he SCA limits its

as the Third Circuit pointed out, courts taking this position are neglecting to consider whether cell phone transmissions fit another definition—wire communications.[200] Admittedly, it seems bizarre to call cell phone transmissions wire communications (since by definition, a cell phone has no wires), however, the statutory definitions found in the SCA lead to a contrary conclusion.[201]

According to the SCA, a wire communication is "any 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 (including the use of such connection in a switching station)."[202] It should be emphasized that by the clear language of this statute, wire communications do not necessarily have to occur *entirely* over wires or cables.[203] Furthermore, because this definition does not exclude tracking devices, it makes no difference whether cell phones are considered tracking devices or not.[204] Therefore, if cell phone transmissions meet the definition of a wire rather than an electronic communication, historical CSLI may be obtained under the SCA without further inquiry.[205]

Calls made or received by cellular phones meet the definition of wire communications for two reasons. First, when making a call, cell phones

application to 'electronic communications,' and specifically states that information from tracking devices is not an 'electronic communication.' . . . CSLI is rather obviously information from a 'tracking device' . . . ."). This case also lists several other cases that have explicitly found or "strongly suggested" that cell phones are tracking devices. 2010 Texas Opinion, *supra* note 149, at 578.

200. *See* Third Circuit Opinion, *supra* note 147, at 310 ("That historical record is derived from a 'wire communication' and does not itself comprise a separate 'electronic communication.' Thus, even if the record of a cell phone call does indicate generally where a cell phone was used when a call was made, so that the resulting CSLI was information from a tracking device, that is irrelevant here because the CSLI derives from a 'wire communication' and not an 'electronic communication.'").

201. *See* 18 U.S.C. § 2510 (2006).

202. *Id.* § 2510(1).

203. The communication must only occur "in part" in such a way as to meet the definition. *Id.*

204. Because the SCA specifically excludes tracking devices from the definition of an electronic communication, one cannot help but conclude that without this exclusion, nothing would prevent a tracking device from being considered an electronic communication. *See id.* § 2510(12)(C). By the same logic, since tracking devices are *not* specifically excluded from the SCA's definition of a wire communication, it leads to the undeniable conclusion that nothing in the SCA prevents a tracking device from being considered a wire communication under the right circumstances. *See id.* § 2510(1). This argument is further bolstered by the fact that both definitions appear in the same section of the same chapter of the United States Code. *Id.* § 2510(1), (12).

205. *Id.* § 2510(1).

certainly facilitate aural transfers.[206] Second, as discussed above, cell phones make use of switching stations to connect calls from one cell phone to another cell phone or telephone.[207] Classifying cell phone calls as wire communications is significant because, under the SCA, records (including historical CSLI) can be obtained absent a warrant pertaining to *either* electronic communications *or* wire communications.[208] So, as long as historical CSLI fits the statutory definition for either of these, the SCA applies and the government therefore has the statutory authority to request such information.[209] Treating cell phone transmissions as electronic communications under the SCA has proven to be controversial, but treating these transmissions as wire communications is a more appropriate classification.[210]

Though it may seem strange to classify calls from a cell phone as wire communications, this interpretation is not a new one.[211] In fact, in addition to the Third Circuit, other courts have come to the same conclusion.[212] Moreover, the legislative history suggests that one of Congress's objectives in implementing the Electronic Communications Privacy Act in 1986 was to broaden the definition of wire communications to include cell phones.[213] Despite all this, some advocates for a probable cause standard in applications for historical CSLI insist that calls from a cell phone are electronic, rather than wire communications.[214] However, these arguments are usually based on a highly selective reading of the SCA.[215] These

206. To qualify as a wire communication, the communication must have some aural component. *Id.*

207. *See supra* note 37 and accompanying text.

208. 18 U.S.C. § 2703(d) (2006).

209. *Id.* However, even if the government has the *statutory* authority to request historical CSLI, the Fourth Amendment could still require probable cause, because the Fourth Amendment always protects people against unreasonable searches and seizures. U.S. CONST. amend. IV.

210. *See supra* notes 199–209 and accompanying text; *infra* notes 211–16 and accompanying text.

211. *See* John R. Kreese, *Privacy of Conversations over Cordless and Cellular Telephones: Federal Protection Under the Electronic Communications Privacy Act of 1986*, 9 GEO. MASON L. REV. 335, 342 (1987) (concluding that the 1986 amendment which added language about switching stations to the definition of wire communications was intended to bring cell phones under its scope).

212. State v. Serrato, 176 P.3d 356, 360 (Okla. Crim. App. 2007). In fact, this Oklahoma court took its ruling one step further and decided that not only did cell phones fall under the current definition of wire communication, but they also fall under the more restrictive definition that preceded the current one because, simply, cell phones "use wire and cable connections when connecting calls." *Id.*

213. Kreese, *supra* note 211, at 342.

214. *See supra* note 199 and accompanying text.

215. One court clearly misstated the statute when it said the SCA is "limited to information pertaining to wire or 'electronic communications,' which are expressly defined to exclude communications from a device 'which permits the tracking of the movement of a person or object.'" W.D. Pa. Opinion, *supra* note 24, at 601. The judge here did not acknowledge that the definition of wire communication does *not* exclude information from a tracking device. *See* 18 U.S.C. § 2510(1)

arguments fail in light of the overwhelming weight of legal precedent and legislative history that clearly indicates that cell phone calls are wire communications.[216]

There is one last point to address here. As has already been observed, wire communications must involve "aural transfers."[217] This precludes CSLI that might be collected when a phone registers with a cell tower, sends a text message, or utilizes mobile Internet service because none of these involve sound.[218] Thus, only CSLI associated with incoming or outgoing phone calls could be classified as coming from a wire communication.[219] This problem is easily dealt with by law enforcement, who already commonly limit requests for historical CSLI to information that is gathered when a person either makes or receives a call.[220] This ensures the CSLI is gathered as part of a wire communication rather than an electronic communication.[221]

Regardless of how one analyzes the issue, it is clear that the SCA generally, and 18 U.S.C. § 2703(d) specifically, applies to historical CSLI.[222] However, the battle being waged over statutory interpretation of the SCA is only one piece of the puzzle. There is another issue at play that is far more familiar to and cherished by many Americans: the Fourth Amendment.

B. Disclosure of Historical CSLI Is Not a Search Under the Fourth Amendment

Even if the disclosure of historical CSLI can be compelled by the SCA, the Fourth Amendment could preclude the disclosure of such information without a warrant.[223] Warrants may be issued only upon a showing of probable cause, a considerably higher standard than the "specific and

---

(2006). Commentators have also made this mistake. One author emphasized the words "wire, cable, or other like connection" in section 2510 to support his conclusion that "cellular communications . . . clearly are not a form of wire communication." Chamberlain, *supra* note 27, at 1757. This is puzzling, because, as discussed above, the part of the statute that ensures cell phones fall under the definition of wire communications is the language about "switching stations." *See supra* note 211.

216. *See supra* notes 212–13.

217. 18 U.S.C. § 2510(1) (2006).

218. Third Circuit Opinion, *supra* note 147, at 310 (finding that CSLI came from a wire communication only when a "subscriber makes a cellular phone call").

219. *Id.*

220. *Id.* In this case, the government requested CSLI consisting only of information collected when the phone in question was either making or receiving a call. *Id.*

221. *See supra* notes 218–19.

222. *See supra* notes 162–218 and accompanying text.

223. This is a constant refrain among privacy advocates. *See* Isikoff, *supra* note 11, at 40.

articulable" facts standard outlined in the SCA.[224] So, whether a warrant is necessary hinges on whether or not the disclosure of historical CSLI is a "search" under the Fourth Amendment. If it is a search, a warrant for that information must be obtained upon a showing of probable cause.[225] Application of the two-pronged *Katz* test[226] below shows that the disclosure of historical CSLI is not a search.

1. The First *Katz* Prong: Do Cell Phone Users Have a Subjective Expectation of Privacy in Their Location?

At one time, courts believed that a physical trespass by law enforcement was a prerequisite to finding that a search had occurred under the Fourth Amendment.[227] *Katz v. United States* signaled and abandonment of this line of thinking when the Court declared that the Fourth Amendment protects "people, not places," and introduced the two prong test used today to analyze whether an action is a search.[228] The first prong of the test that must be satisfied if information is to be protected by the Fourth Amendment is whether the person in question has a *subjective* expectation of privacy in the information.[229] This prong is typically easily satisfied because the assertion that one had a personal expectation of privacy in the information is supported by the nearly invisible infrastructure cell phones utilize to provide users with service.[230]

Although people often do have a subjective expectation of privacy in their location, even this subjective expectation is sensitive to contextual factors such as where people are and what they happen to be doing with their cell phones.[231] For instance, if, in the course of a conversation, a person explicitly mentions to another party where he is currently located, that

224. *See supra* note 66 and accompanying text.

225. U.S. CONST. amend. IV. Though the general rule is that a search requires a warrant based on probable cause, there are a number of exceptions to this requirement. *See generally Warrantless Searches and Seizures*, 35 GEO. L.J. ANN. REV. CRIM. PROC. 37, 37–127 (2006) (surveying the numerous exceptions to the warrant requirement). However, courts ruling on requests for historical CSLI based on less than probable cause seem to assume that none of these exceptions apply. *See, e.g.*, W.D. Pa. Opinion, *supra* note 24, at 611 ("It appears to this Court . . . that this information is entitled to the judicial-review protections afforded by a probable cause warrant and historically applied to movement/location information derived from a tracking device.").

226. *Supra* notes 74–76 and accompanying text.

227. Katz v. United States, 389 U.S. 347, 352–53 (1967).

228. *Id.* at 351.

229. *See* California v. Ciraolo, 476 U.S. 207, 211 (1986).

230. *See* Isikoff, *supra* note 11, at 40. Privacy advocate James X. Dempsey claims that most people "don't have a clue" that their cell phone company can track them in real time (or, by extension, historically). *Id.*

231. *See infra* notes 232–36 and accompanying text.

person cannot claim to have a subjective expectation of privacy.[232] Similarly, GPS devices are used in a host of applications for smartphone devices.[233] For example, Google Latitude is just one of many applications that, if someone chooses, will display her location on a map for all of her chosen friends to see either on their smartphone devices or computer.[234] Someone utilizing an application such as this cannot claim any subjective expectation of privacy.[235] Thus, this prong should not be entirely overlooked, as both prongs of the *Katz* test must be met for behavior to qualify as a search under the Fourth Amendment.[236]

2. The Second *Katz* Prong: Is a Cell Phone User's Expectation of Privacy as to That User's Location Reasonable?

Assuming that a cell phone user has a subjective expectation of privacy in his or her location, that expectation must still be reasonable.[237] Although the Supreme Court has not provided any guidance when it comes to CSLI specifically, the Court did provide some insight in *Knotts* and *Karo* into the relatively limited circumstances in which a person may have a reasonable expectation of privacy in his or her location.[238]

a. Cell Phone Users Have No Objectively Reasonable Expectation of Privacy Outside of Private Residences

In *Knotts*, the Supreme Court noted that "[n]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them."[239] Shortly thereafter, the Court in *Karo* ruled:

232. This would fall under the Third Party Doctrine. *See infra* notes 264–278 and accompanying text.

233. *E.g.*, *GPS Phone Carriers Assume Possible Risk and Reward*, TARGETED NEWS SERVICE (Jan. 7, 2011), http://targetednews.com/pr_disp.php?pr_id=3177171.

234. *Google Latitude*, GOOGLE MOBILE, http://www.google.com/mobile/latitude/ (last visited Jan. 10, 2012).

235. Recall that in *Smith v. Maryland*, the defendant lost his reasonable expectation of privacy because he dialed a number on the telephone. *See supra* note 83. Broadcasting one's location via a phone application would likely have a similar effect.

236. *Supra* note 74 and accompanying text.

237. *Supra* note 76 and accompanying text.

238. *See supra* notes 88–98 and accompanying text.

239. United States v. Knotts, 460 U.S. 276, 282 (1983).

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time.[240]

In making these statements, the Supreme Court gave guidance to law enforcement officials using new and advanced forms of electronic surveillance—the focus is not on the type of surveillance or how it is used, but rather on the target of the surveillance and whether that person is observable from a public place.[241] This distinction between public and private locations is well understood, even by courts that have ruled that historical CSLI requests require probable cause:

> Taken together, these cases establish that without a warrant based on probable cause the Government may use a tracking device to ascertain an individual's location on a public highway but not in a private home, *i.e.*, the public/private dichotomy is the principle harmonizing *Knotts* and *Karo*, so that a warrant is constitutionally required if and only if the location information extends onto private property.[242]

However, at least one magistrate judge repudiated this well-settled distinction between public and private locations when she said: "what an individual seeks to preserve as private, and thus free from inspection, though it may be in a public area, may nevertheless be outside of the government's reach."[243] This summation of Fourth Amendment protections elevates the importance of the first, subjective *Katz* prong so much so that it eviscerates the second, objective prong.[244] This is evidenced by the fact that the court

240. United States v. Karo, 468 U.S. 705, 716 (1984).

241. "Public place" may be too restrictive. As long as a law enforcement officer could *conceivably* determine a person's location "by visual observation made from a spot where one is legally permitted to be," there is no Fourth Amendment violation. M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1457 (2007). This logically follows from *Knotts* and *Karo*, because if someone is exposing his or her location to *any* member of the general public, courts will not recognize a reasonable expectation of privacy in that person's location. *Id.*

242. W.D. Pa. Opinion, *supra* note 24, at 613.

243. Massachusetts Opinion, *supra* note 178, at 74, *rev'd sub nom*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

244. *See id.* In any Fourth Amendment search analysis, both prongs of the *Katz* test must be satisfied. *See supra* notes 74–76 and accompanying text.

did not analyze the second prong at all in its opinion.[245] This court's approach is entirely antithetical to Supreme Court precedent, and worse, has been relied on by commentators arguing for a probable cause standard, advancing a confusing and unworkable Fourth Amendment interpretation.[246]

Proponents of a warrant requirement for obtaining historical CSLI cite the Supreme Court of Washington's *State v. Jackson*[247] decision to advance the argument that Fourth Amendment protections can extend into the public sphere when surveillance represents an "invasion into private lives" and the disclosure of "intimate details."[248] This case carries little weight, however, because the Washington State constitution is more protective than the Fourth Amendment,[249] and nothing in *Knotts* or *Karo* suggests expectations of privacy as to location extends to the public realm *at all*.[250]

Thus, as the law stands, if a person is observable "from a spot where [a law enforcement officer] is legally permitted to be," no Fourth Amendment

245. *See* Massachusetts Opinion, *supra* note 178, *rev'd sub nom*, *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

246. *See* Chamberlain, *supra* note 27, at 1784. Chamberlain's argument focuses on a distinction between information from one's past and present, and uses this case in support of his conclusion that a person's reasonable expectation of privacy of presence at a certain location does not vanish simply because that person left that location. *Id.* However, the relevant inquiry is not if a reasonable expectation of privacy was *lost*, but rather, if that person ever had it in the first place. *Supra* notes 74–76 and accompanying text. Contrary to Supreme Court precedent, both Chamberlain and the Massachusetts court discussed here assume that "if an individual wishes not to disclose information about the destinations to which she *will be traveling*, that individual maintains a privacy interest in guarding against disclosure of those destinations *even after having gone to and left them*." Chamberlain, *supra* note 27, at 1784. However, according to *Knotts* and *Karo*, when it comes to one's location, it is what a person *does* disclose that determines whether the Fourth Amendment has been violated, not merely what that person *wishes* to disclose. *See supra* notes 84–102.

247. 76 P.3d 217 (Wash. 2003).

248. *See* Koppel, *supra* note 78, at 1075. In his argument, Koppel inexplicably decides that "[t]hough the Jackson court did not rely upon the Supreme Court's Fourth Amendment case law, its focus on the potential intrusiveness of the technology was entirely consistent with the directive of the *Katz* line of cases." *Id.* at 1074. This argument is flawed for two reasons. First, Washington's constitution is more protective than the Fourth Amendment, because it extends protection explicitly to one's "private *affairs*." *See supra* note 193. Second, this argument is manifestly *inconsistent* with *Knotts*, in which the Supreme Court decided that the manner or extent of surveillance is irrelevant as long as "[v]isual surveillance . . . *would have* sufficed to reveal [all facts gathered from technological surveillance]." United States v. Knotts, 460 U.S. 276, 282 (1983) (emphasis added).

249. WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."). The Fourth Amendment, of course, does not contain language regarding private affairs, but instead guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV.

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

protections apply.[251] The next section explores whether historical CSLI represents an invasion of privacy when someone is in an area in which he *does* hold an objectively reasonable expectation of privacy.

b. Historical CSLI Does Not Intrude upon a Person's Reasonable Expectation of Privacy Even when a Person Is in a Private Residence

Many insist that because historical CSLI may communicate to the police the contents of a home, the warrantless gathering of this information is a search and thus a violation of the Fourth Amendment.[252] This is indeed problematic because it is clear that people—cell phone users or otherwise—enjoy a reasonable expectation of privacy as to their locations if they are within their homes.[253] Some have argued that because people typically carry their cell phones with them at all times (including while at home), historical CSLI "cannot help but implicate the home" and thus should be obtainable only with a warrant.[254] However, people have an expectation of privacy only in things that are on the inside of their homes, and historical CSLI does not convey information about the interior of a home.[255]

---

251. Clark, *supra* note 241, at 1457.

252. *See* Chamberlain, *supra* note 27, at 1788.

253. United States v. Karo, 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the *Fourth Amendment* to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time." (emphasis added)).

254. Koppel, *supra* note 78, at 1086–87. The author goes on to state without supporting authority that "it would be exceedingly difficult to only track a suspect while he was outside the home." *Id.* at 1087. However, the government often limits the scope of the information it requests from a cell phone company. *See* Indiana Opinion, *supra* note 26, at *1 (analyzing a request for CSLI limited to information gathered during incoming or outgoing calls). *See also* Elise M. Simbro, Comment, *Disclosing Stored Communication Data to Fight Crime: The U.S. and EU Approaches to Balancing Competing Privacy and Security Interests*, 43 CORNELL INT'L L.J. 585, 598 (2010) ("[C]ourts emphasized the limited scope of the [historical CSLI] requested; law enforcement authorities were not seeking to activate GPS capabilities on the target's phone in order to track the target in real time or track the location of the phone when it was not being used."). In some situations, the government could simply exclude from its request information from any tower within range of the user's residence.

255. In considering the issue of historical CSLI, the Third Circuit recounted the testimony of FBI Agent William B. Shute from a different trial. Third Circuit Opinion, *supra* note 147, at 311. In analyzing historical CSLI, Agent Shute would only go so far as to say the data indicated that it was "highly possible" that the user was at home or that the user was "in the vicinity of her home." *Id.* The Third Circuit also acknowledged that Agent Shute would not state that the historical CSLI was "reliable evidence" that a user was at home. *Id.* at 312. After recounting this testimony, the Third Circuit turned to the case before them and found no evidence that historical CSLI "extends to [the] realm" of a private residence. *Id.* at 313. Without question, historical CSLI is strong circumstantial evidence that a cell phone user was at or near a certain location at a certain time—otherwise, it would have very little value to law enforcement. *Id.* at 312 ("CSLI may, under certain

In *Karo*, the beeper was precise enough to "indicate[] that the beeper was inside the house."[256] In contrast, as previously discussed, historical CSLI can usually indicate the location of a cell phone to within about 200 feet.[257] Unless a person is standing in the middle of a residence and the walls are 100 feet away in any direction, his historical CSLI will not be precise enough to prove that he is actually inside the walls of the residence and secluded from the public eye.[258] Even in the best case scenario, a phone equipped with a GPS device might be located to within fifty feet, which would rarely be precise enough to say with certainty that a phone is located within the walls of any residence.[259] The most that could be said is that it produces a "genuine probability" that the phone is inside the residence.[260]

The difference between a high probability and a certainty may seem trivial, but the Third Circuit recognized the distinction was "not irrelevant"

---

circumstances, be used to approximate the past location of a person."). However, it is simply not precise enough to convey with total certainty the "actual whereabouts" of a person. *See id.*

. 256. United States v. Karo, 468 U.S. 705, 715 (1984).

257. *Supra* note 52 and accompanying text.

258. In his article, Chamberlain imagines "a cell phone user who, carrying her phone, moves from one end of her palatial private residence to another" and states that this imaginary user would offend the principles of *Karo*. Chamberlain, *supra* note 27, at 1788. This would be correct, as long as the CSLI indicates a radius entirely within the walls of the residence. *Karo*, 468 U.S. at 715. However, the average size of a single-family residence in 2001 was 2553 square feet. *Square Footage Measurements and Comparisons: Caveat Emptor*, EIA: RESIDENTIAL (May 22, 2003), http://www.eia.doe.gov/emeu/recs/sqft-measure.html [hereinafter *Square Footage Measurements and Comparisons*]. In contrast, according to the formula πr^2, the area of a circle with a radius of 100 feet is about 31,416 square feet. Obviously, houses come in all shapes and sizes, and these measurements do not necessarily reflect the considerable variation in possible measurements, but the huge difference in coverage area indicates that Chamberlain's hypothetical "palatial residence" is a rare one indeed. Chamberlain, *supra* note 27, at 1788. Thus, in the exceedingly rare situation that CSLI does indicate a person is entirely within the walls of a residence, the issue should be litigated in the "more appropriate context of a motion to suppress." *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007). As discussed above, cell phones located using their GPS devices can be located much more accurately (within fifty feet), which could indicate the presence of a phone entirely within the walls of a residence—and thus possibly infringe on a person's Fourth Amendment rights—with much greater frequency than other types of CSLI. *Supra* note 55 and accompanying text. However, law enforcement agencies could easily avoid such dangers by simply opting not to request GPS information.

259. The average size of a single-family residence in 2001 was 2553 square feet. *Square Footage Measurements and Comparisons*, *supra* note 258. Based on the formula πr^2, the area of a circle with a radius of fifty feet is about 7853 square feet. A house would have to be quite large for CSLI to actually give information only about the interior of that house.

260. *See* Third Circuit Opinion, *supra* note 147, at 311–12 ("The Government correctly notes that Agent Shute did not state that the cell-site information 'is reliable evidence' that the suspect was at home . . . . Agent Shute only stated that it is 'highly possible' that the user was at home or in the vicinity.").

to its analysis of the Fourth Amendment implications of historical CSLI.[261] This is likely due to *Karo*, in which the Supreme Court found a Fourth Amendment violation because the beeper in that case "reveal[ed] a critical fact about the *interior* of the premises" by signaling to the police that the can of ether it was attached to was hidden inside the house.[262] Conversely, CSLI cannot indicate *with certainty* anything about the interior of a private residence.[263] Thus, the Fourth Amendment does not protect historical CSLI, and current law does not require a warrant or probable cause to obtain historical CSLI.

C. The Third Party Doctrine

There is one final issue to consider when analyzing whether historical CSLI deserves Fourth Amendment protections: the Third Party Doctrine. In *United States v. Miller*, the Supreme Court defined the scope of this doctrine:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[264]

Thus, if, as some courts have determined, this "Third Party Doctrine" applies to CSLI, then the Fourth Amendment is *never* implicated in cases concerning CSLI.[265] Courts often hold that the determining factor for whether the Third Party Doctrine applies is whether the information is "voluntarily" conveyed to the third party.[266] Historical CSLI has been

---

261. *Id.* at 312.

262. United States v. Karo, 468 U.S. 705, 715, 719 (1984) (emphasis added).

263. *Supra* note 255 and accompanying text.

264. United States v. Miller, 425 U.S. 435, 443 (1976).

265. *See, e.g.*, United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. 2008) ("By voluntarily using the equipment, the cell phone user runs the risk that the records concerning the cell phone call will be disclosed to police."). Due to this "risk" that the information will be turned over to someone else, there is no expectation of privacy in the information shared—in this case, historical CSLI. *Id.*

266. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). This focus on whether the action is voluntary is crucial in the second prong of the *Katz* test. *See supra* note 76. Without voluntarily conveying information to a third party, a person may still expect that information to remain private (due to misplaced trust or a number of other reasons), but society would not find that expectation to be reasonable since, of course, the third party would be free to share that information with whomever they like. *See Smith*, 442 U.S. at 743–44.

analogized with other types of personal records, such as bank records, that courts have ruled are "voluntarily conveyed" to a third party.[267]

Courts requiring a probable cause standard often dismiss the idea that the Third Party Doctrine applies because cell phones automatically register with cell phone towers and send location information without any voluntary action by the user.[268] As previously discussed, this is a natural and necessary consequence of owning and using a cell phone.[269] When the Third Circuit ruled on this issue, it stated, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[270] To support this assertion, the court pointed out that cell phone users probably do not know that cell phone companies are collecting and storing CSLI, and thus users cannot knowingly (much less voluntarily) convey such information.[271] There are two problems immediately apparent in this analysis. First, because cell phone use costs vary depending on what country a cell phone user is in, cell phone users must expect that their cell phone company gathers location information with some specificity when determining proper billing charges.[272] Second, as users become more aware of cell phone technology, there will no longer be a widespread lack of knowledge regarding the type of location data cell phone companies routinely collect.[273] If people continue to use their cell phones even after

267. *Suarez-Blanca*, 2008 WL 4200156, at *8 (listing records in which consumers have no reasonable expectation of privacy). Included in that court's list of analogous cases are: United States v. Phibbs, 999 F.2d 1053, 1078 (6th Cir. 1993) (holding people have no expectation of privacy in credit card statements); United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985) (finding no reasonable expectation of privacy in motel registration records); United States v. Hamilton, 434 F. Supp. 2d 974, 979–80 (D. Or. 2006) (finding no reasonable expectation of privacy in employment records); United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) (holding there is no reasonable expectation of privacy in kilowatt usage in electricity utility records).

268. *See, e.g.*, 2005 Texas Opinion, *supra* note 26, at 756.

269. *See supra* note 45 and accompanying text.

270. *See* Third Circuit Opinion, *supra* note 147, at 317.

271. *See id.* The court was persuaded by Electronic Frontier Foundation's amicus brief that argued that cell phone users have no indication when they place a call that their location is being gathered and stored. *Id.*

272. *See, e.g.*, *International Roaming*, T–MOBILE: INTERNATIONAL SERVICES, http://www.t-mobile.com/International/RoamingOverview.aspx?tp=Inl_Tab_RoamWorldwide (last visited Jan. 10, 2012). This website provides information on the differing rates for cell phone use while traveling abroad. *Id.*

273. *See* Matt Hendley, *Technology Leads to 'Surveillance Society,'* STATEPRESS.COM (Oct. 5, 2010, 10:10 PM), http://www.statepress.com/2010/10/05/technology-leads-to-%E2%80%9C surveillance-society%E2%80%9D/. Gary Merchant, a law professor at Arizona State University, noted that the lower your expectation of privacy, the less you are constitutionally protected. *Id.* He also noted that while the older generations of Americans find it "creepy" that one might be able to track the location of friends via their cell phones, young people "love it." *Id.* As people start to

they learn and understand how historical CSLI is gathered and maintained, they will have a much harder time arguing that the CSLI has not been voluntarily conveyed.[274]

Another reason historical CSLI should be considered voluntarily conveyed is that the process of registering or receiving calls (and thus conveying CSLI) is easily prevented by turning a cell phone off.[275] Some commentators have suggested that turning off a cell phone for the purpose of retaining one's privacy is impractical, because "it strips the phone of its ability to receive calls," effectively rendering the device useless for its intended purpose.[276] However, recall that the only place someone may have a reasonable expectation of privacy is inside a home.[277] If cell phone users turn off their cell phones as they enter their homes to stop broadcasting CSLI, they might simply turn to their home telephones or computers for their communications needs.[278] Given this ability to easily stop the transmission of CSLI while at home, the choice to transmit *is* voluntary and thus the Third Party Doctrine applies to bar Fourth Amendment protection.

VI. THE NEGATIVE IMPACTS OF A WARRANT REQUIREMENT

A. Technology and Privacy: Strange Bedfellows

In 1999, Scott McNealy, CEO of computer giant Sun Microsystems, famously uttered the startling statement: "You have zero privacy anyway. Get over it."[279] He was responding to a question regarding online privacy,[280] and his comments garnered plenty of outrage from the general public.[281]

---

expect less privacy in their locations while carrying a cell phone, they lose the ability to mount any defense based on the Fourth Amendment. *Id.*

274. *See* United States v. Starkweather, No. 91-30354, at *1–2 (9th Cir. Aug. 24, 1992). In *Starkweather*, the Ninth Circuit ruled that electricity bills were not protected by the Fourth Amendment because the information contained therein is voluntarily turned over to the utility company. *Id.* In reaching this conclusion, the court analogized electricity bills to telephone and bank records, stating that "[t]he public awareness that such records are routinely maintained . . . negate[s] any constitutionally sufficient expectation of privacy regarding the records." *Id.* at *2 (quoting Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 256 (9th Cir. 1977)).

275. *See supra* note 49 and accompanying text.

276. McLaughlin, *supra* note 50, at 436.

277. *See supra* note 98.

278. *See, e.g.*, *Call Phones from Gmail*, GOOGLE, http://www.google.com/chat/voice/ (last visited Jan. 10, 2012). With a free Gmail account, a user can call any phone in the United States or Canada for free. *Id.* All that is required is an Internet connection. *Id.*

279. Luther Martin, *Was Scott McNealy Right?*, SC MAGAZINE (Feb. 5, 2009), http://www.scmagazineus.com/was-scott-mcnealy-right/article/126910/.

280. James Freeman, *You Have Zero Privacy . . . Get Over It!*, IDEAS IN ACTION WITH JIM GLASSMAN (May 15, 2000, 12:00 AM), http://www.ideasinactiontv.com/tcs_daily/2000/05/you-have-zero-privacyget-over-it.html.

281. Martin, *supra* note 279.

Despite the outrage, Mr. McNealy is not alone in expressing this sentiment,[282] and there is often a disconnect between what people say they want—privacy—and their behavior.[283]

This disconnect is especially apparent in today's cell phone technology.[284] Many functions on a smartphone utilize location information to pinpoint a user's location for a variety of reasons, including reasons indicative of the isolated and lonely nature of modern life, such as a call to other lonely strangers for instant company, revelry, or even a romantic connection.[285] Even more basic cell phone models usually contain some location-based technology, such as turn-by-turn road navigation.[286] To provide these functions, cell phone companies must always determine the user's location to some level of accuracy.[287] It is for this reason, perhaps, that in a recent poll only 16% of Americans thought that their right to privacy was "safe."[288]

---

282. Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get Over It*, TECHNOTICA ON MSNBC.COM (Jan. 13, 2010, 8:56 AM), http://www.msnbc.msn.com/id/34825225/ns/technology_and_science-tech_and_gadgets/. Google's CEO, Eric Schmidt, said in an interview with CNBC, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." *Id.*

283. Martin, *supra* note 279. The author points out that consumers have no problem shopping "at on-line retailers that keep a record [of] every click of the mouse they make and every web page they view." *Id.* In a recent poll, fifty-five percent of users of geolocation services (those services on a cell phone that can be used to share location information with others on the web) said they were concerned about the loss of privacy one suffers by using such services. Sharon Vaknin, *Are You Worried About Geolocation Privacy? (Poll)*, CNET (July 22, 2010, 5:00 AM), http://news.cnet.com/8301-17938_105-20011282-1.html. However, even though many of these services have features that allow users to keep their locations private (by only broadcasting it to specific friends), twenty-nine percent of users do not limit the dissemination of their location information at all and allow it to remain entirely public. *Id.* Others choose to limit what they share to their private network of friends or family. *Id.* However, even those who believe they are keeping their locations private by restricting their activities to "private" networks may be mistaken, as geolocation apps often post location updates to social networking sites like Facebook, where information can be much less secure. *See id.*

284. *See infra* notes 288–92 and accompanying text.

285. For an interesting but brief overview of location-based dating applications for smartphones, see Laurie Davis, *Managing Your Love Life from Your Smartphone*, EFLIRT EXPERT, http://www.eflirtexpert.com/blog/2010/7/20/managing-your-love-life-from-your-smartphone.html (last visited Jan. 10, 2012).

286. *See, e.g.*, *LG Cosmos VN250 (Verizon Wireless)*, PCMAG.COM, http://www.pcmag.com/article2/0,2817,2364056,00.asp (last visited Feb. 8, 2012). The Cosmos is an "entry-level phone." *Id.* While turn-by-turn navigation is not a standard feature of this phone, customers could pay $9.99 a month to utilize this service, meaning that every model is equipped with the necessary GPS technology. *See id.*

287. *See supra* note 34 and accompanying text.

288. Joel Roberts, *Poll: Privacy Rights Under Attack*, CBS NEWS: OPINION (Feb. 11, 2009, 7:06 PM), http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml.

In the same poll, 83% of Americans expressed a negative opinion about companies' collection of customers' personal information,[289] and yet many, if not most Americans routinely share all sorts of information with private companies about their private lives, preferences, and even locations.[290] Most major grocery chains now have discount card programs that serve the real purpose of collecting data about consumers.[291] Online retailers, such as Amazon.com, may automatically track consumers' purchases, the operating system a consumer is using to access their site, and even the number of mouse clicks a consumer performed while browsing the website.[292] While information from grocery store discount cards or online purchases could likely reveal a person's past location (because they need to either be present at a store or using a computer to make purchases), it would have little chance of obtaining Fourth Amendment protection due to the Third Party Doctrine.[293] Paradoxically, courts have singled out historical CSLI as a type of business record that does deserve the full protection of the Fourth Amendment.[294]

Last year, Mark Zuckerberg, Founder and CEO of the most popular social networking site in the world, Facebook, made the decision to make much of a Facebook user's information publicly available.[295] In response to questions about the wisdom of such a decision, Mr. Zuckerberg said, "We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."[296] While one might argue that Facebook is itself driving social change, it seems clear nonetheless that society *is* changing and Americans' private lives *are* much less private.[297] Whether this is a desirable social change is debatable, but

---

289. *Id.*

290. *See infra* notes 295–96.

291. Katy McLaughlin, *The Discount Grocery Cards That Don't Save You Money*, WALL ST. J., Jan. 21, 2003, http://online.wsj.com/article/0,,SB1043006872628231744,00.html.

292. *Amazon.com Privacy Notice*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496 (last visited Jan. 10, 2012).

293. *See supra* note 267.

294. Isikoff, *supra* note 11, at 40.

295. Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy Is Over*, READWRITEWEB (Jan. 9, 2010, 9:25 PM) http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php. The move made every user's "name, profile picture, gender, current city, networks, Friends List, and all the pages you subscribe to . . . publicly available information on Facebook." *Id.*

296. *Id.*

297. *See id.* The author takes a rather strong stand against Zuckerberg's statements, saying, "I don't buy Zuckerberg's argument that Facebook is now only reflecting the changes that society is undergoing. I think Facebook itself is a major agent of social change and by acting otherwise Zuckerberg is being arrogant and condescending." *Id.* However, while this amounts to arguing over whether the chicken or the egg came first, the author does not deny that society *has* changed. *Id.* Notably, not all analysts see the "death of privacy" as a negative occurrence. *See* Tim Leberecht, *Privacy Is Over. Here Comes Sociality*, POP!TECH (Jan. 21, 2010), http://www.poptech.org/blog/

because of the increased use of technology to share personal information, instituting a warrant requirement for historical CSLI may result in arbitrarily providing Fourth Amendment protections to one realm of people's electronic lives while threatening an important government interest in providing for the safety of the public.[298]

B. The Value of Historical CSLI to Law Enforcement

It should come as no surprise that law enforcement views CSLI as a valuable investigatory tool.[299] In response to the "overwhelming" need for CSLI evidence, the FBI has formed a unit called the Cellular Analysis and Survey Team, the sole function of which is to "provide[] technical assistance, case support and training to federal, state and local law enforcement officers around the nation."[300] This sort of support is likely needed to deal with the "thousands" of requests for CSLI made nationwide every month.[301]

While thousands of ex parte requests for cell phone records may seem ominous, law enforcement officers are doing important and valuable things with these requests.[302] There are hundreds if not thousands of examples of

---

privacy_is_over_here_comes_sociality. Bill Thompson, Technology writer for BBC News Online, said the following about the new social norms:

> The enlightenment idea of privacy is breaking apart under the strain of new technologies, social tools and the emergence of the database state. We cannot hold back the tide, but we can use it as an opportunity to rethink . . . how we engage and interact with others and where the boundaries can be put between the public and private. Those of us who are ahead of the curve when it comes to the adoption and use of technologies that undermine the old model of privacy . . . can offer advice and support to those who might be unhappy to have their movements, eating habits, friendships and patterns of media consumption made available to all. But every [social media user] is sharing more data with more people than even the FBI under Hoover or the Stasi at the height of its powers could have dreamed of. And we do so willingly, hoping to benefit in unquantifiable ways from this unwarranted—in all senses—disclosure.

Id.

298. *See supra* note 281 and accompanying text. *See also infra* notes 303–12.

299. *See infra* notes 303–12.

300. Sampson, *supra* note 162, at A01.

301. Isikoff, *supra* note 11, at 40.

302. For example, law enforcement has used historical CSLI to locate a hiker that almost died of hypothermia. *Police Track Cellphone Signal to Find After-Hours Hiker*, CANADA.COM (Mar. 1, 2011), http://www.canada.com/vancouversun/news/westcoastnews/story.html?id=c55324c1-13c6-4cca-8708-9f9efb9f2360. In addition, law enforcement recently uncovered a possible human trafficking scheme due entirely to one man's partial cell phone call. *Call Leads to Possible Human Trafficking Scheme*, THE SACRAMENTO BEE, June 17, 2011, http://www.utsandiego.com/news/2011/jun/17/call-leads-to-possible-human-trafficking-scheme. The call was dropped before the man, who claimed he was being held against his will, could tell the police where he was located. *Id.*

the government utilizing historical CSLI to obtain convictions or locate criminal suspects.[303] Historical CSLI is particularly helpful when suspects are using prepaid cell phones, or when dealing with a criminal who otherwise knows how to "cover his tracks."[304]

Requiring a warrant every time police wish to use historical CSLI would only serve to slow down and frustrate the efforts of officers, who would have to gather more information to meet the more stringent probable cause standard.[305] It has been said that "the Fourth Amendment seeks to balance degrees of intrusion on our civil liberties against degrees of promotion of legitimate governmental interests."[306] As already discussed, the degree of intrusion by the government when it requests historical CSLI is minimal,[307] yet the governmental interest in using this information to deter crime and catch criminals is extremely compelling.[308]

VII. CONCLUSION

Government today is often portrayed as the oppressive "Big Brother": cold, uncaring, and without any respect for individual privacy rights.[309] This characterization is so pervasive, it is even advanced by major news

---

Fortunately, cell phone records led police to the house from which the call came. *Id.* Finally, a FBI special agent had this to say about historical CSLI: "I use it every day and have used it to find hundreds of people . . . . The agents that I have trained have used it to find thousands of people." Sampson, *supra* note 162.

303. In a recent murder trial, historical CSLI was considered to be "important evidence" by jurors discussing the case after handing down a guilty verdict. Terry Katz, *Following Guilty Verdict, Jury Members Discuss the Trial*, STURGISJOURNAL.COM (Mar. 12, 2011), http://www.sturgisjournal.com/community/centreville/x2011262879/Following-guilty-verdict-jury-members-discuss-the-trial. Prosecutors used historical CSLI to prove two parents were not at home asleep, as they claimed, when seven of their four-month-old's fingers were chewed off by a pet ferret. *Parents of Ferret Attack Victim Charged*, KSALLINK.COM (June 16, 2011), http://www.ksallink.com/?cmd=displaystory&story_id=17894&format=html. In another investigation in Kentucky, the suspected sole survivor of a three man shootout during a home invasion claimed he was not at the crime scene on the night in question, but his historical CSLI indicated otherwise. *Deadly Home Invasion Case Sent to Grand Jury*, KYPOST.COM (June 13, 2011), http://www.kypost.com/dpp/news/state/Home-InvasionShooting_17400962.

304. Sampson, *supra* note 162.

305. *Id.* ("[The SCA's standard] is a much lower burden than the probable cause standard required under the Fourth Amendment."). For a helpful and concise chart explaining the different evidentiary standards that police must meet under different circumstances, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620 (2003). To obtain a warrant, the government must establish "a likelihood that a crime has occurred and that evidence of the crime exists in the location to be searched," while a "specific and articulable facts" court order does not require the government to establish a likelihood of anything, and the information must be relevant *to the investigation*, rather than the crime itself. *Id.*

306. W.D. Pa. Opinion, *supra* note 24, at 591.

307. *See supra* Part V.

308. *See supra* note 302 and accompanying text.

309. Isikoff, *supra* note 11, at 40.

outlets.[310] With so much negativity directed toward government action, it is difficult to discern when the government gets it right.

However, Congress has, in the SCA, created a workable test that both protects citizens and provides for the evolving needs of law enforcement agencies. As a threat to constitutional privacy rights, historical CSLI has a bark that is far worse than its bite. Lately, courts and commentators alike have been quick to jump to the conclusion that a warrant must be required before the government can access historical CSLI. These viewpoints seem to be grounded in either a misinterpretation of the statutes that make up the SCA or a vague, but unfounded, belief that this sort of information just *feels* like it should be protected by the Fourth Amendment.[311] While it is imperative that courts help to protect the privacy of people within the United States, a warrant requirement could frustrate the efforts of law enforcement agencies while at the same time extending Fourth Amendment protections to information in which people have no reasonable expectation of privacy. Neither of these results should be palatable to the courts, to law enforcement, or to the public at large. In the future, courts should grant requests for historical CSLI as long as the "specific and articulable facts" standard imposed by the SCA[312] has been met by the government.

Kyle Malone*

310. On his Fox News program Glenn Beck spoke directly to the issue of historical CSLI and the Third Circuit's decision not to require a warrant for historical CSLI: "The FBI and other agencies will now no longer need a search warrant to track your location. They'll use your cell phone. Nobody is going to a judge." *The Glenn Beck Program* (Fox News Network broadcast Sept. 27, 2010). This small bit of misinformation (18 U.S.C. § 2703(d) (2006) *does* require the government to obtain an order from a judge to gain access to CSLI) only serves to fuel the flames of discontent among the public, and shows little appreciation for the delicate balance between individual rights and the needs of law enforcement that courts must attempt to maintain.

311. *See* Third Circuit Opinion, *supra* note 147, at 308. The court recognized that the issue of privacy rights is an emotional one, even to judges, "The MJ erred in allowing her impressions of the general expectation of privacy of citizens to transform [the standard outlined in the SCA to a probable cause standard]." *Id.*

312. 18 U.S.C. § 2703(d) (2006).

* J.D. Candidate, 2012, Pepperdine University School of Law; B.A. in Political Science, 2008, Kansas State University. I would like to thank my family for their love, support, and for always encouraging me to explore the world beyond the comfortable confines of home.