# CHECKING IN: HISTORIC CELL SITE LOCATION INFORMATION AND THE STORED COMMUNICATIONS ACT

*Christopher Fox*[*]

## I. INTRODUCTION

Over the last twenty-five years, the number of cell phone subscribers in the United States has increased from slightly over 200,000 in 1985 to roughly 293 million in 2010.[1] Cell phones are now the only phones used in over one quarter of all American households, a percentage that has nearly tripled in the last five years.[2] Moreover, several modern phones are equipped with GPS programs that allow subscribers to accurately and easily navigate to their destination[3] using the phone that they likely have on or near their person for the majority of the day.

As technology has developed over the last quarter century, the average person's life has changed through the adoption and utilization of new devices. Not only are cell phones regularly used for checking emails or updating one's Facebook status, but the Federal Communications Commission (FCC) estimates that wireless phones are responsible for about seventy percent of all 911 calls.[4] In re-

[*] J.D., May 2012, Seton Hall University School of Law; B.A., 2006, The University of Texas at Austin. I would like to thank the proprietors of El Dubs for consistently giving me gratuitous copies of their daily newspaper with my morning coffee. The Third Circuit decision that is at the heart of this Comment and which piqued my interest in this subject was brought to my attention because of their excellent customer service and appreciation.

[1] *CTIA Semi-Annual Wireless Industry Survey*, CTIA WIRELESS ASS'N, http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf (last visited Nov. 25, 2011).

[2] *Wireless Quick Facts*, CTIA WIRELESS ASS'N, http://ctia.org/media/industry_info/index.cfm/AID/10323 (last visited Mar. 2, 2012) [hereinafter *Wireless Quick Facts*].

[3] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008).

[4] *Wireless 911 Services*, FED. COMMS. COMMISSION, http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html (last visited Mar. 2, 2012); *see also 9-1-1 Statistics*, NAT'L EMERGENCY NUMBER ASS'N, http://nena.siteym.com/?page=911statistics (last visited Mar. 2, 2012) (stating that of the estimated

sponse to this increasing percentage of wireless 911 calls, the FCC has mandated that service providers be able to track ninety percent of wireless 911 calls within 300 meters of the point of origin and within one hundred meters of the point of origin for one-hundred percent of wireless 911 calls by January 18, 2016.[5]

Tracking a cell phone's approximate location from connected calls has also aided the ends of justice on several occasions. A handful of important examples include: recovering a women's stolen car with her five-year-old daughter inside within thirty minutes because the young girl answered her mother's cell phone, which enabled the police to use the cell tower information to locate the vehicle;[6] capturing a fugitive wanted for two murders;[7] leading police to a suspect, who was arrested after a kidnapping and after the murder victim's DNA was found in his car;[8] providing information that contradicted a suspect's statements about his location at home because records showed that his cell phone was used within about three blocks of the place of death of his ex-girlfriend shortly before and after she was shot;[9] and the prosecution's reliance on cell tower record information in the highly publicized Scott Peterson murder trial to contradict Peterson's claim of his whereabouts at a particular time on the morning of his wife's death.[10] In all of these instances, the government used cell site location information (CSLI) to provide an approximation of a subscriber's cell phone location.

Wireless phones are actually sophisticated two-way radios that constantly communicate with nearby cell towers.[11] Through a process

240 million 911 calls annually, one third are wireless calls); *Wireless Quick Facts*, *supra* note 2 (placing the number of emergency 911 calls at over 296,000 per day). As these sources indicate, the percentage of 911 calls attributable to cell phones has consistently and dramatically increased over the last ten years.

[5] 911 Service, 47 C.F.R. § 20.18(h) (2011).

[6] Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 310 (2004) (citing *Girl, 5, Found Safe as Man Steals Car*, ROCKY MTN. NEWS Apr. 22, 2004, at A18).

[7] *Id.* (citing Don Plummer, *Cellphone Betrays Cobb Fugitive*, ATLANTA J.- CONST., Nov. 9, 2003, at A1).

[8] *Id.* (citing Chuck Haga, *Sjodin's Body Found; Officers Find Remains in Ravine Near Crookston*, MINNEAPOLIS STAR TRIB., Apr. 18, 2004, at B1).

[9] *Id.* at 310–11 (citing Holley Gilbert, *Vancouver Man Is Arrested in Shooting Death of Ex-Girlfriend*, PORTLAND OREGONIAN, Apr. 30, 2004, at B1).

[10] *Id.* at 311 (citing Diana Walsh & Stacy Finz, *The Peterson Trial; Defendant Lied Often, Recorded Calls Show; Supporters Misled About Whereabouts*, S.F. CHRON., Aug. 26, 2004, at B1).

[11] *How Wireless Works*, CTIA WIRELESS ASS'N, http://ctia.org/media/industry_info/index.cfm/AID/10324(last visited Mar. 2, 2012) [hereinafter *How Wireless Works*].

known as "registration," a cell phone communicates information identifying the phone, subscriber, and service provider to the cell tower with the strongest signal, which is then relayed to a mobile telecommunications switching office (MTSO).[12] Cellular service providers (CSPs), like AT&T or Verizon, record and maintain CSLI for billing and service purposes in their regular course of business.[13] For example, a CSP determines roaming charges based on the cell site that a subscriber's phone uses for a particular call.[14]

Historic CSLI refers to the records maintained by CSPs that list the cell sites with which a subscriber's cell phone communicated at previous points in time, whereas prospective CSLI refers to the cell sites that a subscriber's cell phone will communicate with at a future point in time and the CSP will correspondingly record. Under the Stored Communications Act (SCA),[15] law enforcement agencies may compel CSPs to disclose prospective or historic CSLI for a particular cell phone in the course of a criminal investigation. Depending on the information that the government seeks, the SCA requires either probable cause and a warrant or reasonable suspicion and a court order for compelled disclosure.[16]

On September 7, 2010, the Third Circuit became the first court of appeals to weigh in on the standard required for a court order to compel CSPs to disclose historic CSLI to law enforcement agencies under § 2703(d) of the SCA.[17] In *In re Application of the United States for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*, an Assistant United States Attorney (AUSA) sought a § 2703(d) order compelling a CSP to disclose a particular subscriber's records in connection with the ongoing investigation of a second individual suspected of drug trafficking.[18] Due to the government's difficulties visually surveying the suspected drug trafficker, the AUSA submitted the application for a § 2703(d) order to

[12] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

[13] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008).

[14] *Id.* at 590 n.20.

[15] 18 U.S.C. §§ 2701–2712 (2006).

[16] § 2703.

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

[18] *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv.*, 534 F. Supp. 2d at 587–88.

aid in the government's counter-drug trafficking operations.[19] The suspected drug trafficker's historic whereabouts could have provided the government with evidence of the location(s) of the suspect's criminal activities.[20] Based on Fourth Amendment privacy concerns formed by the belief that historic CSLI could provide the government intimate details about an individual's life, the magistrate judge denied the government's original request for an order because the law enforcement agency failed to show probable cause for obtaining the historic CSLI from the CSP.[21] When the government appealed the decision to the district court, that court affirmed the decision in a brief two-page opinion based on the finding that the order was "not clearly erroneous or contrary to law."[22]

On appeal, however, the Third Circuit vacated the decision and remanded the case for further proceedings.[23] The Third Circuit interpreted the statute to allow a magistrate judge to exercise discretion in granting § 2703(d) orders because the language of the statute merely sets reasonable suspicion as the minimum requirement for granting an order.[24] Thus, the court did not eliminate the possibility of magistrate judges in the Third Circuit using different standards when considering such orders; it simply established that reasonable suspicion is enough for a judge to grant a law enforcement agency's request for a § 2703(d) order.[25] If a magistrate judge finds that a warrant is required for the § 2703(d) information sought, the magistrate judge must make a finding that "the Government's need . . . for the information [outweighs] . . . the privacy interests of cell phone users" before issuing the order.[26] Because the magistrate judge "never analyzed whether the Government made a showing" of reasonable suspicion, but instead required a showing of probable cause, the court of appeals left the issue for the magistrate judge to determine on remand.[27]

---

[19] *Id.* at 588.

[20] *Id.* at 588 n.12.

[21] *Id.* at 616.

[22] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, No. 07-524M, 2008 U.S. Dist. LEXIS 98761, at *3 (W.D. Pa. Sept. 10, 2008).

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

[24] *Id.* at 312.

[25] *See id.*

[26] *Id.* at 319.

[27] *Id.*

Historic CSLI, however, should not be afforded any Fourth Amendment protection. The Third Circuit's failure to differentiate between historic and prospective CSLI does not clarify the standards that courts should apply to each, nor does it resolve the discrepant standards that magistrate judges use when granting or denying § 2703(d) orders.[28] Instead of analyzing historic and prospective CSLI through the Fourth Amendment jurisprudential lens and then turning to § 2703(d), the Third Circuit focused on interpreting the statutory language of the SCA.[29] Thus, when presented with the opportunity to formulate appropriate guidelines for judges to use for future § 2703(d) order requests from the government, the Third Circuit left the matter unresolved.

Part II of this Comment will explain the process cell phones use for sending and receiving calls, messages, and information, as well as how CSLI data is computed to produce an approximate location of a cell phone. Part III will provide the relevant Fourth Amendment jurisprudence, explain the language and protections provided under the SCA, and examine the Third Circuit's interpretation and application of the statute to a § 2703(d) order request. Part IV will argue that the Third Circuit's cursory analysis of historic CSLI in light of the relevant Fourth Amendment jurisprudence was incorrect, and will highlight the resulting failure to set forth guidelines for § 2703(d) order requests that would end the application of discrepant standards. Finally, Part V will propose an amendment to the statute that will eliminate the current discrepancy and clarify the requirements for compelled disclosure of historic CSLI.

## II. CELL PHONES AND LOCATION APPROXIMATION

The crux of the present issue revolves around historic CSLI. In order to fully comprehend the problematic treatment of historic CSLI and why it is not protected by the Fourth Amendment, one should understand what exactly CSLI comprises and how CSLI is used to calculate approximate location.

### *A. The Technology of Cell Phones*

Cell phones are sophisticated two-way radios that send and receive communications through the nearest cell site.[30] A cell site is the

[28] For a discussion of the discrepant standards that have been applied to § 2703(d) order requests, see *infra* notes 119–21 and accompanying text.

[29] *See infra* Part III.C.

[30] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005).

geographical location containing the cell tower, radio transceiver, and base station controller.[31] Manufacturers program every cell phone with an Electronic Serial Number (ESN), and, additionally, every cell phone is assigned a Mobile Identification Number (MIN) based on the subscriber's phone number.[32] Moreover, the FCC has assigned every CSP a unique System Identification Code (SID).[33] Every cell site broadcasts a control channel,[34] and every cell phone constantly searches for its CSP's control channel to ensure communication with a nearby cell site.[35]

While a cell site is the actual location of the cell tower and accompanying equipment, a cell is the geographical area that is served by three cell sites.[36] Because cell towers are divided into three 120° faces, one cell is served by three cell sites.[37] In turn, each cell site serves three separate cells.[38]

The cell site that communicates with a subscriber's phone will depend on the subscriber's location within that cell.[39] "Registration" is the process whereby a subscriber's cell phone searches for its service provider's SID, selects a control channel for communication with the base station, and then identifies itself to the cell site.[40] This information is then forwarded to the mobile telecommunications switching office (MTSO) and stored in a database, completing the registration process and allowing calls, messages, and information to be directed to the phone.[41] When a call is placed to a subscriber's phone, the MTSO searches the database to locate the cell that the

---

[31] *Id.*

[32] Marshall Brain, Jeff Tyson & Julia Layton, *How Cell Phones Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/cell-phone.htm/printable (last visited Mar. 5, 2012).

[33] *Id.*

[34] *Id.* A control channel is a special frequency used to broadcast a CSP's SID from a base station to a cell phone, which a subscriber's phone searches for whenever it is turned on to ensure communication with one of the subscriber's CSP's cell sites. *Id.*

[35] *Id.*

[36] Tom Farley & Mark van der Hoek, *Cell and Sector Terminology*, PRIVATE LINE (Jan. 1, 2006, 8:55 PM), http://www.privateline.com/mt_cellbasics/index.html.

[37] *See id.*

[38] *Id.*

[39] *See* Tom Farley & Mark van der Hoek, *Basic Theory and Operation*, PRIVATE LINE (Jan. 1, 2005, 9:09 PM), http://www.privateline.com/mt_cellbasics/index.html.

[40] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005). The cell phone identifies itself to the cell site by transmitting its ESN and MIN to the base station. *Id.*

[41] *Id.*

subscriber's phone is in, and then it routes the call through the most recently registered cell site.[42] The registration process occurs approximately every seven seconds when the phone is turned on, regardless of whether the phone is in use, and it ensures the strongest signal strength for the subscriber.[43]

Importantly, the channel that is used for this process is separate from the channel used to transmit the content of calls, messages, or information.[44] When a call is connected to the phone, the control channel used for registration is dropped, and a new voice channel that has been assigned for the call replaces the registration channel.[45] Thus, only the cell site that carried the communication, not the communication itself, is recorded by the CSP.[46]

Furthermore, as a person travels towards the edge of a cell, the original base station notes the decrease in signal strength while the base station the phone is heading towards recognizes an increase in signal strength.[47] The MTSO coordinates a changeover to the new cell site, which the CSP records.[48]

This continuous process aids in seamlessly sending and receiving calls, and it is what allows subscribers to travel several miles while maintaining the same uninterrupted phone conversation.[49] When a cell phone travels outside of a subscriber's home area, another CSP will generally provide service for the subscriber's phone and simply signal the subscriber's home network so that the MTSO knows where to direct incoming calls, messages, or information.[50] Therefore, the subscriber's CSP records and maintains, as a matter of ordinary busi-

---

[42] Brain, Tyson & Layton, *supra* note 32.

[43] *In re Application for Pen Register*, 396 F. Supp. 2d at 750.

[44] *Id.* The significance of this fact is discussed in Part III, *infra*, which argues that the Fourth Amendment does not protect historic CSLI and law enforcement agencies should be able to obtain historic CSLI upon a showing of reasonable suspicion because the channel log does not record any communications; it only evidences the cell sites with which a particular cell phone communicated at certain times.

[45] *In re Application for Pen Register*, 396 F. Supp. 2d at 751.

[46] *See id.*

[47] Brain, Tyson & Layton, *supra* note 32.

[48] *Id.* The second base station facilitates the changeover to the new cell site by sending a signal via a control channel that prompts the subscriber's phone to switch to a new frequency that then carries the call. *Id.*

[49] *See* Farley & van der Hoek, *supra* note 39.

[50] *How Wireless Works*, CTIA WIRELESS ASS'N, http://ctia.org/media/industry_info/index.cfm/AID/10539 (last visited Mar. 5, 2012). This process is known as roaming, and it is what helps expand the areas in which cell phones are operational. *Id.*

ness practice, even the subscriber's cell phone communications with cell sites that other CSPs operate.

### *B. The Methods Used to Approximate Location*

CSPs store a subscriber's registration information in a database so that communications are routed to the user's phone via the closest cell site.[51] While the actual communications are only carried on a single channel from one cell site,[52] the phone's signal is still receivable by more than one cell site.[53] CSLI is the term used to describe the records that CSPs keep regarding which cell sites carried a subscriber's call and which cell sites received the phone's signal. Because more than one cell site usually receives the signal, one can determine the approximate location of the phone by using one of two common methods: Time Distance of Arrival (TDOA) or Angle of Arrival (AOA).[54]

TDOA requires three cell sites to receive the same signal.[55] Because the user is not typically equidistant from all three cell sites, the signal will arrive at each cell site at a different point in time.[56] This time difference is then analyzed and combined with the known coordinates of the three cell sites to generate the estimated latitude and longitude of the phone.[57]

AOA, on the other hand, requires only two cell sites to receive the same signal and is based on calculating the angle at which the signal travelled from a user's phone to the cell site.[58] After determining the angle by which the phone's signal travelled to each cell site, one can determine the approximate location of the cell phone using the known locations of the two cell sites.[59]

TDOA generally produces a narrower estimate of location than AOA, but both provide reliable approximations of a cell phone's lo-

---

[51] For a detailed discussion how cell phones communicate, see *supra* Part II.A.

[52] *See supra* text accompanying notes 45–46.

[53] *See Time Difference of Arrival Location Determination*, DISPATCH MAG. ON-LINE, http://www.911dispatch.com/911/tdoa.html (last visited Mar. 5, 2012) [hereinafter *Time Difference of Arrival Location Determination*].

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *AOA–Angle of Arrival*, TRUEPOSITION, http://www.trueposition.com/aoa (last visited Mar. 5, 2012) [hereinafter *AOA–Angle of Arrival*].

[59] *Id.*

cation.[60] Both of these forms of location approximation do not require adding anything to a cell phone because all of the calculations are based on the recorded signal information that the phone sends out and the known coordinates of the receiving cell sites.[61] Thus, one can determine the general area of a cell phone's location by simply using information that CSPs record and store in their regular course of business without modifying or implementing a subscriber's phone in any way.

Some scholars have argued that using TDOA or AOA to determine the past approximate location of a cell phone is an impermissible violation of one's Fourth Amendment privacy rights because it could provide police with information about an individual's location that might otherwise be unobtainable.[62] But this information helps police respond to 911 calls faster, and it can provide valuable information to assist in solving heinous crimes and crimes perpetrated by law enforcement officers.[63] Critics acknowledge the benefits that CSLI provides to law enforcements agencies, however, some still argue that both historic and prospective CSLI should not be obtainable without a showing of probable cause and the issuance of a warrant.[64] Because historic CSLI does not provide the government with the same information that a tracking device produces, and because it is a third party who collects and maintains the information in the regular course of business, the critics' analogies of historic CSLI to tracking devices are incorrect, and the Fourth Amendment concerns purportedly implicated are not constitutionally supported.

---

[60] *U-TDOA-Uplink Time Difference of Arrival*, TRUEPOSITION (last visited Mar. 5, 2012), http://www.trueposition.com/u-tdoa/.

[61] *See AOA—Angle of Arrival*, *supra* note 58; *see also Time Difference of Arrival Location Determination*, *supra* note 53.

[62] *See, e.g.*, Patrick T. Chamberlain, *Court Ordered Disclosure of Historic Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1752, 1788 (2009) (arguing that locational data gleaned from CSLI, historic or prospective, mandates Fourth Amendment protection); Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 317 (2004) (arguing that the Fourth Amendment should apply to CSLI).

[63] Peter J. Sampson, *Cellphones Give Feds Insight into Criminal Activity*, NORTHJERSEY.COM (Jan. 18, 2011), http://www.northjersey.com/news/114072489_Feds_dialed_in_to_criminals.html?page=all.

[64] *See* sources cited *supra* note 62.

## III. THE FOURTH AMENDMENT AND THE STORED COMMUNICATIONS ACT

### *A. Relevant Fourth Amendment Jurisprudence*

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[65] As a threshold matter, Fourth Amendment protections apply only when there is a "search" or "seizure."[66] Justice Harlan's concurrence in *Katz v. United States* set forth a two-prong test to determine whether a search has occurred.[67] The test requires that an individual first "exhibit[] an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[68] Thus, for an individual to successfully claim that a Fourth Amendment "search" has taken place, he or she must harbor a personal expectation of privacy in the information, and that personal expectation of privacy must be shared by an objective, reasonable person.[69] If either prong is not satisfied, then a search has not taken place, and the Fourth Amendment's protections are not implicated.[70]

Section 2703 of the SCA permits the government to search subscribers' records.[71] The Supreme Court has examined the government's search of an individual's records in the past, but has not directly ruled on § 2703. In 1976 in *United States v. Miller*, the Court addressed whether a Fourth Amendment search occurred when the government compelled two banks to disclose a customer's records.[72] In *Miller*, government agents presented subpoenas to the presidents of the two banks requiring the production of all records of accounts in Miller's name.[73] The banks complied with the government's request without advising Miller about the subpoenas.[74] All records were

[65] U.S. CONST. amend. IV.

[66] *Id.*

[67] 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[68] *Id.*

[69] *Id.*

[70] *See id.*

[71] 18 U.S.C. § 2703 (2006).

[72] 425 U.S. 435, 442–43 (1976) (finding no expectation of privacy in bank records because there is an inherent risk that the information an individual gives to the bank will be relayed to the government).

[73] *Id.* at 437.

[74] *Id.* at 438.

made available to the agents, as well as copies of any documents that the agents wished to have.[75]

Although Miller argued that a reasonable expectation of privacy existed in the information he provided to the banks, the Court held that the compelled disclosure of Miller's financial records from the two banks did not constitute a Fourth Amendment search.[76] The Court found that the Fourth Amendment did not provide privacy protection for an individual's bank records because the documents were "business records of the banks."[77] The bank was a party to all of Miller's transactions that were disclosed to the government,[78] the checks represented "negotiable instruments to be used in commercial transactions," and the deposit slips and financial statements represented voluntarily conveyed information.[79] Thus, Miller "possessed no Fourth Amendment interest" because the compelled disclosure of the information was not a search, eliminating the need for a reasonableness assessment or a warrant to obtain the financial information.[80]

Underlying the Court's rationale in this decision was the "assumption of the risk" doctrine, which is premised on the fact that, when one voluntarily provides information to a third party, one assumes the risk that the information may be disclosed to the government.[81] Three years later, the Court used the same rationale for pen registers. In *Smith v. Maryland*, the Court addressed "the question whether the [government's] installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment."[82] The Court distinguished the use of a pen register from a listening device because pen registers "do not acquire the *contents* of communications"; they merely acquire the numbers dialed.[83] The Court used this determination to characterize the defendant's argument as a "claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[84]

---

[75] *Id.*

[76] *Id.* at 442–43.

[77] *Id.* at 440.

[78] *Miller*, 425 U.S. at 440–41.

[79] *Id.* at 442.

[80] *Id.* at 445.

[81] *Id.* at 443.

[82] 442 U.S. 735, 736 (1979). A pen register is a "mechanical device that records the numbers dialed on a telephone." *Id.* n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)).

[83] *Id.* at 741.

[84] *Id.* at 742.

In evaluating the subjective expectation of privacy prong, the Court noted that "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[85] Furthermore, the Court declared that, even if Smith had a subjective expectation of privacy, this expectation was not objectively reasonable.[86] Returning to the "assumption of the risk" doctrine used in *Miller*, the Court held that dialed numbers constituted "information . . . voluntarily turn[ed] over to third parties," in which courts have consistently denied an expectation of privacy.[87] Because the "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information[,] . . . . [he] assumed the risk that the company would reveal to police the numbers he dialed."[88] Thus the warrantless use of a pen register to record the numbers that Smith dialed did not constitute a search under the Fourth Amendment.[89]

Shortly thereafter in a pair of cases decided in consecutive terms, *United States v. Knotts*[90] and *United States v. Karo*,[91] respectively, the Court addressed the use of tracking beepers by law enforcement agencies to determine the location of chemicals suspected of being used for drug production. Employing the use of beepers allows law enforcement agents to track the object the beeper has been attached to by following the emitted signals,[92] similar to the way in which one can compute historic CSLI to create a general picture of the movements of a cell phone, but with greater accuracy and in real-time.

In *Knotts*, law enforcement agents installed a tracking beeper in a drum of chloroform suspected of being used to manufacture drugs

[85] *Id.* at 743.

[86] *Id.*

[87] *Id.* at 743–44.

[88] *Smith*, 442 U.S. at 744.

[89] *Id.* at 745–46.

[90] 460 U.S. 276, 285 (1983) (holding that no Fourth Amendment search occurred when the government used a tracking beeper because the information it provided could have been obtained by following the drum of chloroform's public movements). A tracking beeper is a "radio transmitter . . . which emits periodic signals that can be picked up by a radio receiver." *Id.* at 277.

[91] 468 U.S. 705, 715 (1984) (holding that a Fourth Amendment search did occur when the government's use of a tracking beeper revealed information about the interior of a home that was unobservable from a public place).

[92] *See Knotts*, 460 U.S. at 278.

and traced the drum to a secluded residence using the beeper.[93] The Court noted that the record did not show that the beeper was used again once the signal indicated that the drum was stationary and located in the area of the secluded residence.[94] The agents then used the beeper transmissions and the information obtained from visual surveillance of the residence to secure a search warrant.[95]

The Court held that the use of the beeper in *Knotts* did not constitute a Fourth Amendment search because law enforcement did not invade any reasonable expectation of privacy.[96] Sitting outside of the residence, the drum was observable from public places, and it travelled from the point of purchase to the residence over public roads.[97] The information that the beeper provided would have been ascertainable by "[v]isual surveillance from public places . . . . 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."[98] The Court also reiterated that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[99] Thus, no search had taken place because the information gleaned from the beeper was no different than information that law enforcement agents could have obtained by observing the public movements of the drum of chloroform.[100]

The following term, the Court revisited law enforcement agents' warrantless use of tracking beepers. In *Karo*, police placed a tracking beeper inside a container of ether that they suspected was going to be used to extract cocaine from clothing.[101] Law enforcement agents used the beeper, along with visual surveillance, to follow the ether from the point of purchase to a residence, but use of the beeper did not end once the location of the residence was known.[102] The police continually used the beeper over a prolonged period of time to track the ether, and determined its location to be inside different private

[93] *Id.* at 277–78.
[94] *Id.* at 278–79.
[95] *Id.* at 279.
[96] *Id.* at 285.
[97] *Id.* at 282.
[98] *Knotts*, 460 U.S. at 282.
[99] *Id.* at 281.
[100] *Id.* at 285.
[101] United States v. Karo, 468 U.S. 705, 708 (1984).
[102] *Id.*

residences on multiple occasions.[103] Part of the information that the agents provided to obtain a search warrant for the final residence was the tracking beeper's location.[104]

The Court distinguished the facts of *Karo* from those in *Knotts*. The *Karo* Court noted that the agents conceded that the tracking beeper was used to locate the can of ether inside a particular private residence.[105] The question presented, therefore, was "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[106] Because the beeper provided the police with information not ascertainable by visual surveillance from outside the curtilage of the home, the Court held that the Fourth Amendment privacy interest that an individual has in his or her private residence was violated.[107] Thus, the Court drew a public/private dichotomy when analyzing the Fourth Amendment implications of warrantless use of a tracking beeper.

### *B. The Language and Protections of the Stored Communications Act*

The SCA regulates access to stored wire and electronic communications information and transactional records.[108] The SCA describes the procedures available to law enforcement agencies to obtain this information and clearly creates two separate, exclusive categories: information and records that contain the contents of communications[109] and information or records that do not contain the contents of communications.[110] Section 2703 prescribes the procedures that the government must follow to obtain information containing the contents of communications in electronic storage,[111] information containing the contents of communications in a remote

[103] *Id.* at 708–10.

[104] *Id.* at 709–10.

[105] *Id.* at 714.

[106] *Id.*

[107] *Karo*, 468 U.S. at 715 ("[The beeper] reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.").

[108] Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2006).

[109] § 2703(a)–(b) (providing the requirements for compelled disclosure of the *contents* of wire or electronic communications in electronic storage and a remote computing service, respectively).

[110] § 2703(c) (providing the requirements for compelled disclosure of "record[s] or other information pertaining to a subscriber . . . (not including the contents of communications)").

[111] § 2703(a).

computing service,[112] and records in electronic storage or a remote computing service that do not include the communications' contents.[113]

A law enforcement agency may compel disclosure of information that does not include the content of the communications if the agency meets the guidelines of § 2703(c).[114] There are three different means by which a law enforcement agency may compel a CSP to disclose a subscriber's CSLI: the agency may "obtain[] a warrant,"[115] "obtain[] a court order for such disclosure under subsection (d),"[116] or get "the consent of the subscriber or customer to such disclosure."[117]

Specifically, a § 2703(d) "court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation."[118] Therefore, a law enforcement agency's showing of reasonable suspicion is enough for a court to grant a governmental entity's § 2703(d) order request. The government is not statutorily required to show probable cause in order to obtain a court order compelling a CSP to disclose a subscriber's records.

In practice, however, judges do not always uphold this standard. The same district in New York has applied two different standards to § 2703(d) requests by the government. A magistrate judge denied an application for a § 2703(d) order compelling disclosure of historic CSLI due to "the Fourth Amendment requir[ing] the government to obtain a warrant, based on a showing of probable cause on oath or affirmation, in order to secure" the historic CSLI sought.[119] The opinion acknowledged that the information sought was limited to historic CSLI for a specified period, but the court held that such information was protected by the Fourth Amendment.[120]

---

[112] § 2703(b).

[113] § 2703(c).

[114] *Id.*

[115] § 2703(c)(1)(A).

[116] § 2703(c)(1)(B).

[117] § 2703(c)(1)(C).

[118] § 2703(d).

[119] *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MJ-0550, 2010 U.S. Dist. LEXIS 88781, at *2 (E.D.N.Y. Aug. 27, 2010).

[120] *Id.* at *13.

At the other end of the spectrum, a district court judge granted the government's § 2703(d) order request to compel a CSP to disclose prospective CSLI after presenting "specific and articulable facts showing reasonable grounds to believe that the information sought [wa]s relevant and material to an ongoing criminal investigation."[121] These two cases, both from the Eastern District of New York, are a perfect example of the discrepant standards that currently exist for § 2703(d) order requests by the government. This illustrates the lack of uniformity in the application of a single statutory provision.

Historic CSLI is content free, and reveals the cell site with which a cell phone communicated during a call, not the information that was communicated during a call.[122] Still, historic CSLI must fall within the scope of the SCA for § 2703 to compel CSP disclosure. When applying the SCA, courts must read the definition of certain SCA terms using the definitions that Congress gave to the identical terms under § 2510.[123] Because the SCA only applies to "stored wire and electronic communications," the threshold question is whether the information sought constitutes wire communications or electronic communications as defined by § 2510.[124]

### *C. Judge Sloviter's Opinion's Interpretation and Application of the SCA*

Commentators have argued that cell phones do not send or receive wire communications[125] because the transfer of information is not "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."[126] While it is true that a cell phone operates as a radio,[127] in *In re*

[121] *In re* Application of the U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008); *see also In re* Application of the U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (stating, after granting a § 2703(d) order for prospective CSLI based on only a showing of reasonable suspicion, that it would reveal the cell phone's "general location—and in some circumstances, permit law enforcement agents to track the precise movements—of a particular cellular telephone on a real-time basis").

[122] *See supra* Part II.B (describing that CSLI is information that pertains to the cell site the wireless phone communicated with, not the actual content of a call, message, or information that was sent or received by the wireless phone).

[123] 18 U.S.C. § 2711(1) (2006).

[124] *Id.* § 2703.

[125] *See* Chamberlain, *supra* note 62, at 1757 (arguing that the cell phones are automatically excluded from wire communications because of their wireless operation).

[126] 18 U.S.C. § 2510(1) (2006).

*Application of the United States for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*, Judge Sloviter affirmed that CSLI "consists of records of information collected by cell towers when a subscriber makes a cellular call. That historical record is derived from a 'wire communication' and does not itself comprise a separate 'electronic communication.'"[128]

Electronic communication, the other category of information obtainable under the SCA, is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio*, electromagnetic, photoelectronic or photoptical system."[129] The definition, however, excludes four types of communications that would otherwise qualify,[130] one of which is "any communication from a tracking device" as defined by § 3117.[131]

A tracking device is "an electronic or mechanical device which permits the tracking of the movement of a person or object."[132] Thus, commentators have also argued that the compelled disclosure of historic CSLI based on the SCA alone pursuant to a § 2703(d) order requires a showing of probable cause and a warrant because a cell phone meets the statutory definition of a tracking device and is therefore excluded from the SCA.[133] This argument, however, overlooks the fact that "the Senate Report on the ECPA, which encompasses the SCA, defines 'electronic tracking devices' as 'one-way radio communication devices that emit a signal on a specific radio frequency . . . [that] can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder.'"[134] Since cell phones are sophisticated two-way radios,[135] unlike the devices described in the Senate report, the tracking device definition of §

[127] *How Wireless Works*, *supra* note 11.

[128] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 (3d Cir. 2010).

[129] § 2510(12) (emphasis added); *see How Wireless Works*, *supra* note 11 (explaining that cell phones are sophisticated two-way radios).

[130] § 2510(12)(A)–(D).

[131] § 2510(12)(C).

[132] § 3117(b).

[133] *See, e.g.*, Chamberlain, *supra* note 62 at 1775–77 (arguing that a cell phone falls under the statutory definition of a tracking device, and therefore the SCA prohibits compelled disclosure of historic CSLI absent a showing of probable cause).

[134] *In re* Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't , 620 F.3d 304, 309 n.4 (3d Cir. 2010) (quoting S. REP. NO. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564).

[135] *How Wireless Works*, *supra* note 11.

3117(b) does not encompass cell phones. Thus, historic CSLI is not excluded from the SCA because historic CLSI qualifies as a record of electronic communications.[136]

Furthermore, under the definition of CSLI as a wire communication,[137] even if a cell phone was considered a tracking device, the government could still compel CSP disclosure because the tracking device exclusion only applies to stored electronic communications, not stored wire communications.[138] Thus, Judge Sloviter's opinion correctly held "that CSLI from cell phone calls is obtainable under a § 2703(d) order and . . . such an order does not require the traditional probable cause determination."[139] Instead, the reasonable suspicion language in the text of § 2703(d) is the minimum standard that applies to a § 2703(d) order request.[140]

This finding, however, was not the end of the Third Circuit's statutory examination of § 2703(d). Upon a closer reading of the statute, the court revealed that the language employed in § 2703(d) seemingly sets reasonable suspicion as the floor, but allows for the exercise of judicial discretion in requiring a higher standard.[141] Section 2703(d) clearly states that "[a] court order for disclosure under subsection (b) or (c) *may be issued* by any court that is a court of competent jurisdiction and *shall issue only if*" reasonable suspicion is met.[142] Focusing first on the "may be issued" language, the court stated that it was "the language of permission, rather than mandate. If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever . . . [reasonable suspicion] is met, Congress could easily have said so."[143] The court went on to declare that "[a]t the very least, the use of 'may issue' strongly implies court discretion."[144]

---

[136] *In re Application for an Order Directing a Provider of Elec. Commc'n Serv.*, 620 F.3d at 312–13.

[137] *Id.* at 310

[138] 18 U.S.C. § 2510(1) (2006); *see also supra* text accompanying notes 129–32 (explaining that tracking devices are excluded from the statutory definition of electronic communications).

[139] *In re Application for an Order Directing a Provider of Elec. Commc'n Serv.*, 620 F.3d at 313.

[140] *Id.* (quoting the standard provided in the text of § 2703(d) as requiring "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").

[141] *Id.* at 315.

[142] 18 U.S.C. § 2703(d) (2006) (emphasis added).

[143] *In re Application for an Order Directing a Provider of Elec. Commc'n Serv.* , 620 F.3d at 315.

[144] *Id.*

Noting this discretionary language, the court examined the "only if" language next.[145] Relying on a previous Third Circuit decision, the court articulated that the "phrase 'only if' describe[s] a necessary condition, not a sufficient condition, and that while a 'necessary condition describes a prerequisite,' a 'sufficient condition is a guarantee.'"[146] Therefore, according to the Third Circuit, the statute does not require a judge to issue a § 2703(d) order compelling a CSP to disclose a record upon a showing of reasonable suspicion by the government, but rather it is the minimum requirement that must be met for such an order to issue.[147]

Thus, Judge Sloviter's opinion correctly found that historic CSLI is obtainable under § 2703(d) of the SCA regardless of whether one characterizes historic CSLI as an electronic communication or a wire communication. Because cell phones are not included in the tracking device definition of § 3117(b), historic CSLI is not one of the four types of electronic communications excluded from being obtainable under the SCA. Additionally, historic CSLI is derived from a wire communication because it is a record collected by a cell tower. Thus, historic CSLI is obtainable under a § 2703(d) order upon the statutorily required showing of reasonable suspicion, and the traditional probable cause determination is not required.

## IV. CSLI, FOURTH AMENDMENT JURISPRUDENCE, AND MISINTERPRETATION OF JUDGE SLOVITER'S OPINION

While the court's statutory interpretation and application are generally sound, the court's cursory Fourth Amendment analysis of historic CSLI was incorrect. The Fourth Amendment does not protect historic CSLI. By leaving that possibility open, Judge Sloviter's opinion will not eliminate the discrepant standards that judges apply to § 2703(d) order requests. While the court did not hold that the Fourth Amendment protects historic CSLI, it allowed a magistrate judge to make such a finding in the future.[148] Should the magistrate so find, "a full explanation that balances the Government's need (not

[145] *Id.*

[146] *Id.* at 316 (quoting Township of Tinicum v. U.S. Dep't of Transp., 582 F.3d 482, 488–89 (3d. Cir. 2009)).

[147] *See id.* at 316–17 (reiterating the Third Circuit's previous interpretation of identical statutory language, accepting the EFF brief's argument that this creates a "sliding scale," and rejecting the government's argument that the language provides for mandatory issuance of an order if reasonable suspicion is shown).

[148] *Id.* at 319.

merely desire) for the information with the privacy interests of cell phone users" is necessary.[149]

Curiously, the court rejected the "assumption of the risk" doctrine as applicable to CSLI based on the finding that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[150] The "assumption of the risk" doctrine was the underlying rationale that the Supreme Court used in deciding both *Miller* and *Smith*.[151] Here, the court relied on the Electronic Frontier Foundation's (EFF) brief's claim that cell phone subscribers are unlikely to be aware that a CSP records historical CSLI.[152] This assertion is inapposite to the Supreme Court's rationale in the *Smith* decision.

In *Smith*, the telephone customer was presumed to know that the phone company would record, for business purposes, the numbers he dialed on his telephone.[153] Furthermore, the Court explicitly held that the dialed numbers were information voluntarily conveyed to a third party.[154] The same reasoning and rationale apply directly to cell phone subscribers and historic CSLI. CSPs record CSLI for business purposes, and a cell phone customer should similarly be presumed to know that this information will be recorded because CSPs use it to determine roaming charges that appear on a subscriber's monthly statement.[155] Thus, the roaming charges on the billing statement indicate to the subscriber that the physical location of the phone during a call is known and recorded by the subscriber's CSP in its regular course of business. Thus, by using the cell phone the subscriber voluntarily conveys to the CSP the phone's general geographical location.

Additionally, the prevalence of cell phones with GPS functions and subscribers' increased use of these services[156] directly undermine the position that cell phone customers are not "voluntarily" sharing their location information with CSPs. Therefore, a cell phone user

---

[149] *In re Application for an Order Directing a Provider of Elec. Commc'n Serv.*, 620 F.3d at 319.

[150] *Id.* at 317.

[151] *See supra* text accompanying notes 81, 87–88 (describing the "assumption of the risk" doctrine and its application to the facts of *Miller* and *Smith*).

[152] *In re Application for an Order Directing a Provider of Elec. Commc'n Serv.* , 620 F.3d at 317.

[153] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[154] *Id.* at 743–44.

[155] *See supra* notes 13–14 and accompanying text.

[156] *See supra* note 1–3 and accompanying text.

has no legitimate expectation of privacy in the CSLI that the CSP records when the user makes or receives a call because the subscriber has voluntarily shared this information with the CSP and assumes the risk that the CSP may turn the information over to law enforcement agencies. Moreover, cell phone subscribers who simply pay their monthly bills without looking at them and who do not have GPS functions on their phones are still likely to know that the government uses such techniques due to the high-profile crimes that law enforcement agencies have reported and solved with the help of CSLI.[157]

Furthermore, when analyzing CSLI, courts must apply the public/private dichotomy that the *Knotts* and *Karo* decisions created. In *Knotts*, the Court emphasized the fact that law enforcement agents only used the tracking beeper to follow the movements of a drum of chloroform on public thoroughfares until they determined that the drum had come to rest in the area of a secluded residence, at which time they discontinued the use of the tracking beeper and visually confirmed the presence of the drum of chloroform *outside* the residence.[158] The Court was quick to distinguish these facts in *Karo*, in which law enforcement agents used the tracking beeper to confirm the presence of a can of ether *inside* multiple residences, on multiple occasions.[159] The Fourth Amendment protections afforded to the home made the warrantless use of a tracking beeper that revealed otherwise unascertainable information and that was conducted from outside the curtilage of the residence unconstitutional.[160]

Moreover, CSLI requires different treatment than tracking beepers because CSLI does not provide the precise location information of a cell phone, but it does provide the CSP with the cell site that helped carry a call.[161] This information does not provide the actual location of the cell phone because CSLI only gives the cell tower location used to carry a call and because location calculations based on cell towers give only an approximation of a subscriber's phone's location.[162] If multiple cell sites record CSLI, the approximate location of the cell phone at the initiation of the call can be computed.[163] This approximate location, however, provides the general area of the

[157] *See supra* notes 6–10 and accompanying text.
[158] United States v. Knotts, 460 U.S. 276, 278–79 (1983).
[159] United States v. Karo, 468 U.S. 705, 708–10 (1984).
[160] *Id.* at 715.
[161] *See supra* notes 60–62 and accompanying text
[162] *See supra* notes 54–59 and accompanying text
[163] *See supra* notes 54–59 and accompanying text

caller, not the exact location.[164] A tracking beeper, on the other hand, can be traced to a precise location.[165] Thus, even using TDOA or AOA,[166] historic CSLI cannot show that a subscriber was at a particular place at a particular time; it can only show that the phone was in the general area.

In light of these two characteristics, CSLI falls outside of the traditional Fourth Amendment protections. Accordingly, when a law enforcement agent uses voluntarily conveyed historic CSLI information to approximate a subscriber's location, it does not constitute a Fourth Amendment search. Thus, the necessary "search" or "seizure" required for applying the Fourth Amendment protections[167] is not met when CSPs disclose historic CSLI to a law enforcement agency, but Judge Sloviter's opinion's failure to make this determination has left magistrate judges without a definitive guideline for granting § 2703(d) orders.

Admittedly, the statute provides for judicial discretion in granting § 2703(d) orders, but had the Third Circuit thoroughly analyzed the Fourth Amendment's application to historic CSLI, it would have held Fourth Amendment protections inapplicable to historic CSLI and curbed judicial discretion in granting § 2703(d) orders for this particular type of information. As it currently stands, a judge may require probable cause for a § 2703(d) order requesting historic CSLI if the privacy interests of the cell phone user outweigh the government's need for the information.[168] A finding that cell phone subscribers do not have a privacy interest in historic CSLI would have eliminated the possibility for discrepant application of standards in § 2703(d) order requests for historic CSLI.

## V. PROPOSED STATUTORY AMENDMENT

Because Judge Sloviter's opinion has not alleviated the possibility of magistrate judges applying discrepant standards to § 2703(d) requests, which results directly from the permissive statutory language, a statutory amendment is well overdue. Eliminating the "only if" language from § 2703(d), as well as changing "may be issued" to "shall

[164] *See supra* notes 54–60 and accompanying text

[165] *See* United States v. Knotts, 460 U.S. 276, 277 (1983).

[166] For a discussion of the TDOA and AOA methods for determining approximate location of a cell phone, see *supra* notes 54– 61 and accompanying text

[167] U.S. CONST. amend. IV; *see also supra* text accompanying note 65.

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

be issued" would correct the current problem. An amended version of § 2703(d) would then read:

> A court order for disclosure under subsection (b) or (c) *shall be issued* by any court that is a court of competent jurisdiction and *shall issue if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Although the Fourth Amendment does not protect historic CSLI,[169] the revised statute would still provide a level of judicial oversight that would prevent law enforcement agencies from conducting fishing expeditions. In order for the government to compel a CSP to disclose historic CSLI, courts would still require specific and articulable facts showing that there are reasonable grounds to believe that the contents of the records sought are relevant and material to an ongoing criminal investigation. Thus, unless the government can provide a judge with information showing reasonable suspicion that a subscriber's cell phone records are material to on ongoing criminal investigation, a § 2703(d) order would not be granted.

Alternatively, if Congress believes that cell phone users have a strong privacy interest in historic CSLI, Congress should entirely eliminate the § 2703(d) order requirement from the SCA, and courts should apply the probable cause or subscriber-consent standards required by § 2703(a)–(c). Although the heightened requirement would provide a greater burden on the ability of law enforcement agencies to compel disclosure of historic CSLI, at least the application of the statute would be uniform. Currently, some citizens are erroneously granted Fourth Amendment privacy rights for their historic CSLI, while others are denied Fourth Amendment protection for their prospective CSLI.[170] The Fourth Amendment does not apply to historic CSLI, leaving the statute as the only applicable protection. Therefore, an amendment to § 2703(d) is necessary to ensure that courts apply uniformly the protections that the SCA affords to historic CSLI.

## VI. CONCLUSION

To date, the Third Circuit is the first and only appellate court to weigh in on the appropriate standard for § 2703(d) order requests.

---

[169] *See* discussion supra Part IV.

[170] *See supra* notes 119–21 and accompanying text.

While the court's statutory analysis concerning the definitions and applicability of § 2703(d) order requests to historic CSLI was correct, unfortunately, Judge Sloviter's opinion failed to analyze the applicability of the Fourth Amendment to historic CSLI. By neglecting to highlight the constitutional distinction between prospective and historic CSLI, the Third Circuit's holding will likely fail to remedy the discrepant standards that courts have applied to the government's § 2703(d) order requests.

Because of the ever-increasing dependence on cell phones by citizens in their day-to-day lives and by the government for solving crimes and providing services, the problem of discrepant application of standards for § 2703(d) order requests is sure to persist. Absent a rapid increase in circuit court litigation that creates a split in authority on the matter that may prompt the Supreme Court to grant certiorari, a congressional amendment to the statute is the only available remedy to this problem in the near future.

Historic CSLI is only protected by the SCA, not the Fourth Amendment. Probable cause is neither statutorily nor constitutionally mandated for the disclosure of historic CSLI to law enforcement agencies. Because, as demonstrated in this Comment, the problem will likely not find a solution in the courts, the impetus is on Congress to amend the statute to ensure equal application of § 2703(d)'s provisions. While Judge Sloviter's opinion attempted to address and resolve the issue, ultimately the problem remains largely unchanged because it failed to address whether the Fourth Amendment applies to historic CSLI. Had the Third Circuit performed this analysis, the discretionary language of § 2703(d) would have been rendered moot.

The usefulness and benefits of historic CSLI to law enforcement agents conducting criminal investigations is readily apparent. The Fourth Amendment does not protect historic CSLI, but Judge Sloviter's opinion failed to make this finding and distinguish historic CSLI from prospective CSLI. Thus, absent a circuit court holding historic CSLI is not protected by the Fourth Amendment or a statutory amendment by Congress, judges nationwide may still incorrectly grant historic CSLI Fourth Amendment privacy protections and continue to apply discrepant standards to § 2703(d) order requests by the government. Unfortunately, the Third Circuit clarified the issue, but failed to resolve it, and the hope now is that Congress will amend the SCA and end the discrepant application of the statute.