Washington and Lee Law Review

Volume 68 | Issue 4 Article 7

Fall 9-1-2011

CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment

Steven M. Harkins

CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment

Steven M. Harkins*

Table of Contents

* Candidate for J.D., Washington and Lee University School of Law, May 2012.

I. Introduction

> I was confronted with an application . . . on my first day of criminal duty. . . . for something called "cell site information." Reluctant to sign what I did not understand, I turned to the United States Code and encountered ECPA for the first time. The experience was frustrating: the terminology was unfamiliar, the organization not intuitive, and the syntax far from straightforward. The casenotes accompanying the statute shed no light; they cited only a handful of lower court decisions not particularly relevant to my questions. No appellate court had ever addressed the issue. I asked my colleagues on the bench, and found they were just as puzzled as I was. I tried to look at sample orders from other courts, but found that they were sealed. I met (several times) with AUSAs, who basically argued that their request should be granted because other judges had done so.[1]

United States Magistrate Judge Stephen W. Smith, in written testimony to Congress, concisely summarized the frustrating state of the law regarding cell site information disclosure orders.[2] Perhaps such confusion would be acceptable if law enforcement rarely requested this information or if the privacy interests at stake were limited, but estimates place the number of electronic surveillance orders issued at the federal level alone in excess of 10,000,[3] and the United States is rapidly approaching 300 million cellular phone users.[4] The proliferation of cellular phones and the tenuous protection granted to the location information these phones

---

1. *See Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 81–85 (2010) (written testimony of Hon. Stephen W. Smith, United States Mag. J.) [hereinafter *Smith ECPA Reform Testimony*] (describing the magistrate judge's experience dealing with requests for "prospective" or "real time" CSLI disclosure requests and the different considerations that arise when handling requests for "historical" CSLI).

2. *See id*. (summarizing his experiences with CSLI disclosure cases and discussing the published decisions by other magistrate judges on the issue).

3. *See id*. at 80 ("A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.").

4. *See* CTIA-The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* (2010), http://ctia.org/ (last visited Nov. 23, 2011) (estimating that as of June 2010 there were 292,847,098 cell phones in use in the United States) (on file with the Washington and Lee Law Review).

transmit raises the question, as one commentator put it, of just who knows where you've been?[5]

Approximately every seven seconds, your cellular phone communicates with the nearest cellular tower.[6] This process is called registration, and its primary purpose is to continuously update the cellular network on your location: By identifying the nearest tower, the network can quickly route any incoming call through that tower instead of having to locate your phone mid-call.[7] However, under the Stored Communications Act (SCA),[8] registration can serve a very different purpose.[9] By gathering a sequential history of this cell site location information (CSLI), it is possible for the government to determine the whereabouts of your cell phone within approximately 200 feet every seven seconds.[10]

The Third Circuit Court of Appeals, deciding an issue of first impression in the U.S. Courts of Appeals,[11] found that, under the SCA and

---

5. 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, 308 (2004) (introducing the issue by posing questions such as "[w]hat information *should* be available to law enforcement?").

6. *See In re* 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, 589–90 (W.D. Pa. 2008) [hereinafter Pennsylvania 2008 Opinion] ("Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network and scanning for the one that provides the strongest signal/best reception. This process, called 'registration', occurs approximately every seven seconds.") [vacated language].

7. *See* Radio-Electronics.com, *Mobile Phone Network Registration*, http://www.radio-electronics.com/info/cellulartelecomms/cellular_concepts/registration.php (last visited Nov. 15, 2010) (discussing the need for a registration system for the cellular network to function and noting that "[e]ven when the mobile is in what is termed its idle mode it will periodically communicate with the network to update its position and status") (on file with the Washington and Lee Law Review).

8. *See* Stored Communications Act, 18 U.S.C. §§ 2701–11 (2006) (regulating the acquisition by law enforcement of user account information stored by private parties in the ordinary course of business).

9. *See id.* § 2703(c)(1) (providing for when "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service").

10. *See Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 590 (describing the ability of cell phone towers to place a phone's location within 200 feet in urban areas).

11. *See In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315 (3d Cir. 2010) [hereinafter Third Circuit Opinion] (concluding that "the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d)"); *id.* at 319 (finding that the Stored Communications Act "as presently written gives the [reviewing

the Fourth Amendment, the government need not show probable cause in order to obtain CSLI.[12] Instead, the court found that the government need only provide "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought . . . [is] relevant and material to an ongoing criminal investigation";[13] the court did add, however, that the statute allowed the reviewing judge the option of requiring a warrant showing probable cause.[14] The law is greatly unsettled in this area, with many district courts drawing their own lines, focusing on whether the CSLI sought was historical or prospective.[15] The Third Circuit,

---

judge] the option to require a warrant showing probable cause"). In *Third Circuit Opinion*, the Third Circuit Court of Appeals considered an issue of first impression among the circuit courts: Whether a court may deny the government's application for information under 18 U.S.C. § 2703(d) once the government has satisfied that Section's burden of proof. *Id.* at 305–06. The court specified that the government's request was limited to "information pertaining to a subscriber" contained in § 2703(c). *Id.* at 306. Pursuant to 18 U.S.C. § 2703(d), the government may obtain this information based on a showing of "specific and articulable facts establishing reasonable grounds" that the information sought is "relevant and material to an ongoing criminal investigation." *Id.* at 308. The court determined that CSLI was a "wire communication," not an "electronic communication," and as such even if a cell phone is deemed a tracking device CSLI was not excluded by the SCA's disclosure provision prohibiting inclusion of "electronic communications" obtained from a tracking device. *Id.* at 310. Looking to Congress's intent, the court concluded that the standard for disclosure under § 2703(d) was meant to be lower than the probable cause required for tracking devices because "cell site information provides only a rough indication of a user's location at the time a call was made or received." *Id.* at 312–13. Thus, the court held that CSLI could be obtained under § 2703(d) and that probable cause need not be shown to require the disclosure. *Id.* at 313. The court then proceeded to consider whether magistrate judges have the discretion to require a probable cause warrant on a case-by-case basis. *Id.* at 315. The court found the statute's language established a necessary, but insufficient, condition for disclosure of the requested information. *Id.* at 316–17. Based on this interpretation, the court found that as written the statute gave the Magistrate Judge the option to require a showing of probable cause in any individual case, while recommending that this option be used "sparingly." *Id.* at 319. Appling these principles to the present case, the court vacated the magistrate judge's order denying the government's application, and remanded the application to the district court for a determination of whether the government had satisfied the "specific and articulable facts" that are "relevant and material" standard. *Id.*

12. *See id*. at 315 ("[W]e conclude that the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d) . . . .").

13. *Id.* at 319 (quoting 18 U.S.C. § 2703(d)) (internal quotations omitted).

14. *See id.* ("[T]he statute as presently written gives the M[agistrate] J[udge] the option to require a warrant showing probable cause.").

15. *See, e.g.*, *In re* the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification No. (585) 111-1111 and the Disclosure of Subscriber and Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) [hereinafter New York Feb. 2006 Opinion] (accepting,

as the first federal court of appeals to rule on the issue, will likely influence future decisions in other circuits.[16]

The difference between traditional "probable cause" warrants and the standard required for information disclosure under the Stored Communications Act, 18 U.S.C. § 2703(d) provides substantially different protection for the targets of CSLI requests.[17] This Note considers whether the Third Circuit decision, allowing prosecutors to obtain CSLI without a showing of probable cause, contravenes the Fourth Amendment's guarantee against unreasonable searches and seizures.[18] This Note proposes that it does.[19] The Third Circuit based much of its decision on incorrect

---

in dicta, the Government's interpretation of SCA as authorizing it to obtain historical CSLI); *In re* the Application of U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006) [hereinafter Wisconsin Opinion] (concluding, in dicta and without analysis, that the Government's request for prospective CSLI requires probable cause because it requested prospective rather than historical information); *In re* an Application of U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 303 n.6 (E.D.N.Y. 2005) [hereinafter New York Oct. 2005 Opinion] (stating, in dicta and without explanation, that § 2703(d) "plainly allows" the Government to seek historical CSLI); *In re* Application for Pen Register and Trap/Trace Device With Cell Site Location Auth., 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) [hereinafter Texas 2005 Opinion] (stating, in dicta, that were the communication service providers to compile the tracking information themselves, it would bring the information "more comfortably" within the scope of the Stored Communications Act).

16. *See Third Circuit Opinion*, 620 F.3d at 305–06 ("This appeal gives us our 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."); *see also* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (concluding that the Government does not have the authority to require the disclosure of "cell-phone-derived movement/location information . . . absent a showing of probable cause"), *vacated*, 620 F.3d 304 (3d Cir. 2010).

17. *Compare* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (defining probable cause to exist where "the facts and circumstances within [the officers'] knowledge and of which they [have] reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has or is being committed" (internal quotations omitted)), *with Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 588 (denying the government's request for CSLI regarding an individual not suspected of criminal activity but who purportedly associates with a "Criminal Suspect" on a showing of "specific and articulable facts" under 18 U.S.C. § 2703(d)), *vacated*, 620 F.3d 304 (3d Cir. 2010).

18. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched and the persons or things to be seized.").

19. *See infra* Part VI ("[B]ecause CSLI will almost always reveal information about

assumptions regarding the technology at issue,[20] and thus, under certain circumstances, the substantive holding requires lower courts to follow procedure that is not justified by the Third Circuit's own rationale.[21] After clarifying the functionality and potential uses of the technology at issue, this Note argues that, based on existing precedent and the Third Circuit's own rationale, in almost all CSLI disclosure cases the information obtained is protected by the Fourth Amendment and therefore a showing of probable cause should be necessary to obtain CSLI.

Part II begins by providing some basic information on cellular phone technology and the way CSLI is gathered specifically, and then discusses the distinctions between historical, prospective, and real time CSLI.[22] Part III.A lays out the background to the CSLI disclosure debate, covering first the relevant Fourth Amendment jurisprudence and then discussing the application of several statutes which arguably govern CSLI.[23] In Part III.B,

---

the interior of the home that is protected by the Fourth Amendment, magistrate judges should either require a showing of probable cause, or allow law enforcement to only use CSLI that does not reveal information about the interior of the home.").

20. *Compare* Third Circuit Opinion, 620 F.3d 304, 312 (3d Cir. 2010) (stating "cell site information provides only a rough indication of a user's location *at the time the call was made or received*" (emphasis added)), *with Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 589–90 ("Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network . . . approximately every seven seconds."), *vacated*, 620 F.3d 304 (3d Cir. 2010), *and* Lockwood, *supra* note 5, at 309 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register."), *and* Radio-Electronics.com, *Mobile Phone Network Registration*, http://www.radio-electronics.com/info/cellular telecomms/cellular_concepts/registration.php (last visited Nov. 15, 2010) ("*Even if a call is not made instantly*, the network needs to be able to communicate with the mobile to know where it is." (emphasis added)) (on file with the Washington and Lee Law Review); *compare Third Circuit Opinion*, 620 F.3d at 312 ("CSLI may, under certain circumstances, be used to approximate the past location of a person."), *with Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 590 ("In urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet."), *vacated*, 620 F.3d 304 (3d Cir. 2010).

21. *See Third Circuit Opinion*, 620 F.3d at 315 (concluding that "the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d)"); *id*. at 312 ("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.").

22. *See infra* Part II (providing basic information about cellular networks, cell phone registration, and the distinction between historical and prospective CSLI).

23. *See infra* Part III.A (discussing the definition of a "search" under the Fourth Amendment, analyzing the factors to be considered in making the determination of whether a search has occurred in the CSLI context, and identifying the statutes relevant to CSLI

the general state of the law prior to *In re the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*[24] (*Third Circuit Opinion*) is summarized by briefly analyzing the holdings and rationales of the federal district courts in CSLI disclosure order cases.[25] Part IV discusses the *Third Circuit Opinion* in full detail, focusing on the facts and methodology the court used to arrive at its various conclusions.[26] Then, in Part V, the reasoning discussed in Part IV is revisited and critiqued with reference to the realities of CSLI technology.[27] Finally, on the basis of this analysis, Part VI presents this Note's conclusion regarding the soundness of the *Third Circuit Opinion*'s rationale and recommends a possible approach to handling future CSLI disclosure cases based on existing precedent in light of the breadth of CSLI, which the Third Circuit failed to recognize.[28]

II. A Brief Overview of CSLI Technology

To understand the debate over CSLI disclosure, it is necessary to have some basic knowledge regarding the technology at issue. When a cell phone is turned on, one of the first things that occurs is registration.[29] For the cellular network to function efficiently, the network must be aware of the cell phone's location so it can route incoming calls through the

---

disclosure order cases).

24. *See Third Circuit Opinion*, 620 F.3d at 315 (concluding that "the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d)").

25. *See infra* Part III.B (summarizing several CSLI disclosure case rationales prevalent prior to *Third Circuit Opinion*).

26. *See infra* Part IV (presenting the facts and reasoning used by the court in *Third Circuit Opinion*).

27. *See infra* Part V (discussing *Third Circuit Opinion* by focusing on the court's characterization of CSLI technology and the scope of Fourth Amendment protection as it applies to CSLI).

28. *See infra* Part VI (proposing that magistrate judges should either require a showing of probable cause or require the disclosure order to be minimized in order to exclude the use of location information that places the target inside the home).

29. *See* Radio-Electronics.com, *Mobile Phone Network Registration*, http://www.radio-electronics.com/info/cellulartelecomms/cellular_concepts/registration.php (last visited Nov. 15, 2010) (describing the tasks a cell phone undertakes when it is turned on, and noting that the majority of the process involves registration with the cellular network) (on file with the Washington and Lee Law Review).

appropriate location.[30] Each cell phone has a unique Mobile Identification Number (MIN) and Electronic Serial Number (ESN) that identify it to the cellular network during registration.[31] The cell phone communicates this information to the cell tower whenever it is on, whether or not calls are being made or received.[32] The cell phone must reregister periodically so that a user moving from one place to another will still have calls routed through the nearest base station.[33] This reregistration takes place approximately every seven seconds.[34]

Every tower in a cellular provider's network within range of an active cell phone receives the information sent during registration.[35] To determine which tower is closest to the cell phone, and thus, how to route incoming calls when two towers receive signals from a single phone, the network uses one of two systems to pinpoint the phone's location.[36] A network may use a Time Distance of Arrival (TDOA) system, which determines location by measuring and comparing the time it takes the signal to arrive at each tower.[37] Similarly, an Angle of Arrival (AOA) system measures the angle from which the signal reaches multiple towers, and uses that information to triangulate the cell phone's location.[38] The ability to precisely locate an

---

30. *See id*. (explaining that registration allows the network to "route any calls through the relevant base station as the network would be soon overloaded if the notification of an incoming call had to be sent via several base stations").

31. *See* Lockwood, *supra* note 5, at 309 (describing how the MIN and ESN are assigned to cellular phones and identify them).

32. *See id.* ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

33. *See id*. ("Given the inherently mobile nature of cell phones, units update their registration periodically so that the database is current.").

34. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) ("Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers serving their network and scanning for the one that provides the strongest signal/best reception. This process, called 'registration', occurs approximately every seven seconds."), *vacated*, 620 F.3d 304 (3d Cir. 2010).

35. *See* Lockwood, *supra* note 5, at 308 ("Each tower in a provider's network is equipped with radio intercepts that receive signals from any active cell phone.").

36. *See id*. at 308–09 (explaining how the network uses the registration signal to determine which receiving tower is closest to the phone).

37. *See id*. (noting that the time of arrival allows a single tower to estimate the distance between the tower and the phone, while signals arriving at more than one tower allow the network to use an algorithm based on the this data to calculate the phone's longitude and latitude).

38. *See id.* at 309 ("When multiple towers receive signals, the system can compare the angles of arrival and thus triangulate the relative location of the cell phone.").

individual cell phone is thus predicated largely on the presence of multiple cell towers, which do not exist in some rural areas.[39]

However, in urban environments, providers often maintain a large number of cell towers, and location information obtained from providers in these locations can be very accurate.[40] As noted in *In re the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*[41] (*Pennsylvania 2008 Opinion*), "[i]n urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet."[42] By using more sophisticated methods, like triangulation, the phone can be tracked even more precisely.[43] Thus, because of the inherently mobile nature of cell phones, CSLI can be used to provide detailed information about the location and movement of an individual carrying the device even if that individual never makes a call.[44]

CSLI data is continually collected by telecommunications providers.[45] Requests for disclosure of such collected information can either seek to obtain "historical" CSLI, "real time" CSLI, or both.[46] Because both

---

39. *See id.* (recognizing that in rural areas, "the location information available to providers is significantly less accurate simply because fewer towers are available" to receive a given phone's signal).

40. *See id.* (explaining that the sectioning of towers "into directional 'faces' (north face, south face, etc.)" and the significant number of towers in a relatively small area "gives providers access to quite accurate location information").

41. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (concluding that the Government does not have the authority to require the disclosure of "cell-phone-derived movement/location information . . . absent a showing of probable cause"), *vacated*, 620 F.3d 304 (3d Cir. 2010).

42. *Id.* at 590.

43. *See id*. (discussing how TDOA and AOA triangulation systems as well as determining which face of the tower is receiving the signal can allow providers to more accurately determine the phone's location).

44. *See* Lockwood, *supra* note 5, at 312 ("The reality that people carry their cell phones on their persons means that cell phone tracking technology potentially offers a detailed view of a given subscriber's movements rather than simply providing call-identifying information."); *see also id.* at 309 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

45. *See id.* at 309 ("Even when users are not making calls, cell phones communicate with the nearest cell tower to register.").

46. *See Smith ECPA Reform Testimony*, 111th Cong. 81–85 (2010) (written testimony of Hon. Stephen W. Smith, United States Mag. J.) (describing the magistrate judge's experience dealing with requests for "prospective" or "real time" CSLI disclosure requests and the different considerations that arise when handling requests for "historical" CSLI).

historical and real time CSLI will ultimately be obtained from the telecommunications provider's record of stored information, the distinction between the two from the perspective of the provider is limited—in the first instance law enforcement is given access to the already extant information, and in the second they are given access to the information as soon as it becomes available to the provider.[47] Regardless, the provider is being ordered to disclose stored CSLI data, the only difference being the length of time that the information has been stored.[48]

The historical versus real time distinction becomes important in relation to the privacy interest of the target. Historical CSLI enables law enforcement to reconstruct a person's movements and determine where they were located at a given time prior to the disclosure order.[49] Real time CSLI can be used to actually track the present movements of an individual.[50] "Prospective" and "real time" CSLI are commonly confused as interchangeable,[51] but real time CSLI is actually a distinct subset of prospective CSLI, "which refers to all cell site information that is generated after the government has received court permission to acquire it."[52]

The following hypothetical, adapted from *In re the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site*

---

47. *See id.* at 84–85 (explaining the rationale for viewing historical CSLI as similarly invasive to privacy concerns as real time CSLI); Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 601 (W.D. Pa. 2008) (reasoning that there was no warranted "distinction between real-time ('prospective') and stored ('historic') cell-phone-derived movement/location information"), *vacated*, 620 F.3d 304 (3d Cir. 2010).

48. *See Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 601 (concluding that, from a Fourth Amendment and statutory perspective, historical CSLI is indistinguishable from prospective CSLI and that probable cause is required for both types of information).

49. *See* Lockwood, *supra* note 5, at 311 (describing how a police investigator was able to recreate the suspect's movements by referencing which cell tower picks up a cellular phone's transmissions).

50. *See In re* the Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. on Tel. Nos. [Sealed] and [Sealed] and the Prod. of Real Time Cell Site Info., 402 F. Supp. 2d 597, 599 (D. Md. 2005) [hereinafter Maryland 2005 Opinion] ("'Real time' cell site information refers to data used by the government to identify the location of a phone at the present moment.").

51. *See id.* at 598 n.2 ("The government appears to use the terms 'real time cell site information' and 'prospective cell site information' interchangeably, but the two are distinct.").

52. *Id.* at 599.

Information[53] (*Maryland 2005 Opinion*), illustrates the difference between the three classifications of CSLI: Suppose the government receives an order granting access to both historical and prospective CSLI on Monday (the prospective order permitting the disclosure of all CSLI going forward).[54] Any CSLI records that the government obtains for dates prior to Monday will be historical CSLI.[55] If "[o]n Thursday, the government begins tracking the phone in real time; such information is both prospective and real time CSLI."[56] On Friday, when the government accesses the CSLI records from Tuesday and Wednesday, "such information is prospective but not real time cell site information."[57] In sum, all CSLI that is created after the disclosure order is obtained is prospective CSLI,[58] all CSLI that was in existence prior to the disclosure order is historical CSLI,[59] and only CSLI that is provided in real time to law enforcement after the disclosure order is real time CSLI. The realities of CSLI technology and the type of information to which access is being sought are both important factors to keep in mind when looking at CSLI disclosure order cases.

III. State of the Law Regarding CSLI

A. Origins of the Dispute

There is a long background of Fourth Amendment jurisprudence and numerous statutory provisions that impact the current debate over CSLI

---

53. *See id*. at 605 (finding the government's proffered statutory authority insufficient to authorize an order for cell site information absent a showing of probable cause).

54. *See id.* at 599 n.5 ("For example, imagine the government receives a court order on a Monday granting access to prospective cell site information (i.e. all cell site information generated going forward).").

55. *See id.* at 599 ("Records stored by the wireless service provider that detail the location of a cell phone in the past (i.e.: prior to entry of the court order authorizing government acquisition) are known as 'historical' cell site information.").

56. *Id.* at 599 n.5.

57. *See id.* ("On Friday, the government goes back and accesses the records of the phone's location on Tuesday and Wednesday; such information is prospective but not real time cell site information.").

58. *See id.* at 599 (describing prospective CSLI as "all cell site information that is generated after the government has received court permission to acquire it").

59. *See id.* ("Records stored by the wireless service provider that detail the location of a cell phone in the past (i.e.: prior to entry of the court order authorizing government acquisition) are known as 'historical' cell site information.").

disclosure. Broadly categorized, the electronic surveillance tools available under federal law can be envisioned as falling into four separate categories, each of which requires a specific level of proof on the part of the government.[60] At the lowest end of the spectrum are pen register and trap and trace devices, which may be used based on a showing that the information obtained "is relevant to an ongoing criminal investigation."[61] A slightly higher standard, that the government present "*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," is required by statute for disclosure of stored communications or customer account records.[62] To engage in surveillance activity that is categorized as a "search" or "seizure," the Fourth Amendment requires law enforcement to obtain a warrant supported by probable cause,[63] and the Federal Rules of Criminal Procedure specify how such a warrant is to be obtained.[64] And finally, at the most restrictive end of the spectrum, content-capturing wiretaps are subject to the highest standard, and they may only be used in circumstances where law enforcement has satisfied requirements above and beyond the determination of probable cause.[65]

Looking at these four tiers of electronic surveillance, it is important to note where the standard is governed by constitutional principles, where the obligation is purely statutory, and where these two considerations potentially overlap.[66] Absent a finding that the surveillance at issue

---

60. *See In re* the Application of U.S. for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 572–73 (W.D. Tex. 2010) [hereinafter Texas 2010 Opinion] (outlining the four types of electronic surveillance that federal permits to be used as "criminal investigative tools").

61. 18 U.S.C. § 3122(b)(2) (2006).

62. *Id.* § 2703(d) (emphasis added).

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

64. *See* FED. R. CRIM. P. 41(d) (defining the general standard for issuing a warrant to "search for and seize a person or property or to install and use a tracking device" as "probable cause").

65. *See* 18 U.S.C. § 2516(2) (2006) (listing the specific circumstances, such as "when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs," where interception of wire, oral, or electronic communications will be permitted).

66. *See Smith ECPA Reform Testimony*, 111th Cong. 81–82 (2010) (written testimony

constitutes a search or seizure, the Fourth Amendment is not implicated and law enforcement need only comply with the relevant statutory provision.[67] Where a search or seizure of something in which an individual has a recognizable privacy interest is to occur, the Fourth Amendment generally requires a warrant supported by probable cause.[68] In the realm of constitutionally recognized searches and seizures, statutes may define the procedure for obtaining a warrant[69] or may impose additional obstacles to disclosure.[70] To determine which standard governs CSLI disclosure, the courts have had to attempt to place it within this complex tangle of constitutional jurisprudence and statutory language.[71] At its core, the dispute centers on two questions: First, whether obtaining CSLI is a "search" which must comply with the Fourth Amendment; and, second, if it is not a "search," what statutory provision governs the disclosure of CSLI?

---

of Stephen W. Smith, United States Mag. J.) (identifying the four possible categories of investigative tools authorized under the ECPA and describing the relevant individual determination as deciding "which . . . was the best fit for this type of request").

67. *See* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Laws*, 21 CARDOZO ARTS & ENT. L.J. 381, 387–88 (2003) (noting that while constitutional protection for location information may be very limited and such surveillance by private entities falls "outside the scope of constitutional protection, unreasonable searches and seizures by the government fall under Fourth Amendment jurisprudence").

68. *See* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 84 (4th ed. 2010) (describing the "threshold of the Fourth Amendment" as the question of "[w]hat governmental conduct constitutes a *search* or *seizure* of a *person*, *house*, *paper*, or *effect* and, therefore, triggers Fourth Amendment protection").

69. *See* FED. R. CRIM. P. 41(d) (defining the general standard for issuing a warrant to "search for and seize a person or property or to install and use a tracking device" as "probable cause").

70. *See* 18 U.S.C. § 2703(d) (2006) (requiring the government to produce "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" to obtain disclosure under this subsection).

71. *See Smith ECPA Reform Testimony*, 111th Cong. 3 (2010) (written testimony of Stephen W. Smith, United States Mag. J.) (describing the experience of trying to rule on a CSLI disclosure request as frustrating because "the organization was not intuitive . . . . [t]he casenotes accompanying the statute shed no light . . . [n]o appellate court had ever addressed the issue" and "my colleagues . . . were just as puzzled as I was").

1. What Constitutes a "Search"?

The Fourth Amendment to the U.S. Constitution safeguards the right to be free from unreasonable searches and seizures.[72] The amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and specifies that this right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized."[73]

The debate over precisely what constitutes a "search and seizure" under the Fourth Amendment, and thus is entitled to constitutional protection, began evolving rapidly following the U.S. Supreme Court's decision in *Katz v. United States*.[74] The *Katz* Court rejected the government's assertion that the issue should be determined by analysis of whether or not a telephone booth is a constitutionally protected area, and framed the issue as whether the surveilled area was one in which a person has a right to privacy.[75] The Court succinctly stated that "the Fourth Amendment protects people, not places."[76]

In a concurrence in the *Katz* decision, Justice Harlan articulated the two-prong test for determining whether a "search" is sufficiently invasive to raise Fourth Amendment concerns: (1) The individual claiming the right must have exhibited a subjective expectation of privacy; and (2) the expectation of privacy must be one society views as objectively reasonable.[77] *Katz* established that a warrant supported by probable cause was necessary to obtain information electronically, as well as through a

---

72. *See* U.S. CONST. amend. IV (stating a right to be free from "unreasonable searches and seizures").

73. *Id.*

74. *See* Katz v. United States, 389 U.S. 347, 359 (1967) (holding that a search or seizure must have an "antecedent justification" in order to satisfy the demands of the Fourth Amendment even when that search is conducted electronically).

75. *See id.* at 351 (noting the emphasis placed by both parties on the public or private nature of the telephone booth, and stating that "this effort to decide whether or not a given 'area' viewed in the abstract, is 'constitutionally protected' deflects attention from the [real] problem presented by this case").

76. *Id.*

77. *See id.* at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

physical search.[78] To determine whether electronic surveillance was a search and therefore implicated the Fourth Amendment, later decisions by the Court recognized that Justice Harlan's test—"a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable"[79]—has emerged as the standard.[80]

Following that decision, the Court was left to define precisely what types of electronic information gathering implicate the Fourth Amendment.[81] In *United States v. Knotts*,[82] the Court considered whether information obtained by an electronic beeper concealed in a chemical container purchased by the defendant constituted a search and seizure in Fourth Amendment parlance.[83] The analysis focused on the fact that the information obtained had been gathered from the beeper while the defendant was driving on public highways and could have been observed by law enforcement officials through traditional in-person surveillance.[84] A majority of the Court found this type of surveillance to implicate no Fourth Amendment concerns because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his

---

78. *See* Third Circuit Opinion, 620 F.3d 304, 359 (3d Cir. 2010) (requiring a probable cause warrant or equivalent "antecedent justification" as a constitutional precondition for performing electronic surveillance).

79. United States v. Kyllo, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361).

80. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistent[] with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' . . . .").

81. *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding installation of an electronic tracking device implicated no Fourth Amendment concerns when that device was used to track their vehicles on public highways where they had no reasonable expectation of privacy), *with* United States v. Karo, 468 U.S. 705, 717 (1984) (rejecting the Government's claim that it should be able to use tracking devices to identify an object's location within a private residence absent a showing of probable cause).

82. *See Knotts*, 460 U.S. at 285 (finding that there was "neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment" because defendant had no reasonable expectation of privacy in his movement and location information while on public highways).

83. *See id.* at 277 (describing the electronic surveillance used and stating the issue as "whether such use of a beeper violated respondent's rights secured by the Fourth Amendment to the United States Constitution").

84. *See id.* at 281 (characterizing the government's electronic surveillance in this case as "amount[ing] principally to the following of an automobile on public streets and highways").

movements from one place to another."[85] The *Knotts* analysis thus exempted from Fourth Amendment protection electronic surveillance that revealed details which could have been observed through traditional, non-search surveillance techniques, such as following in a car and monitoring with equipment that merely enhanced the normal faculties of law enforcement.[86]

However, in *United States v. Karo*,[87] the Court clarified that under certain circumstances the location information obtained by a tracking device could invade Fourth Amendment protections.[88] The Court affirmatively answered one of the questions left unresolved after *Knotts*: "[W]hether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance."[89] In *Karo*, surveillance revealed the tracking beeper's location within a private residence.[90] Applying the test articulated in *Katz*, the Court found that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[91] Thus, electronic tracking that reveals details about the interior of a private residence is more invasive than the government's activity in *Knotts*, and absent a warrant supported by probable cause such surveillance constitutes a search in violation of the Fourth Amendment.[92]

---

85. *Id.*

86. *See id.* at 285 (reasoning that although "the beeper enabled law enforcement officials in this case to ascertain [information] . . . when they would not have been able to do so had they relied solely on their naked eyes . . . . scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise").

87. *See* United States v. Karo, 468 U.S. 705, 715 (1984) (finding the location information obtained by use of a tracking beeper to constitute a search where the information revealed details about the interior of a private residence).

88. *See id.* at 714 (distinguishing the facts from those in *Knotts* because the tracking device was used to obtain information regarding a "location not open to visual surveillance").

89. *Id.* at 707.

90. *See id.* at 714 ("This case thus presents the question 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.").

91. *Id.*

92. *See id.* (finding that "the monitoring of a beeper in a private residence . . . not open to visual surveillance[] violates the Fourth Amendment rights" of individuals with privacy interests in the residence).

Most recently, in *United States v. Kyllo*,[93] the Supreme Court stated that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[94] In *Kyllo*, federal agents performed a thermal imaging scan of the defendant's home from a car parked across the street from the defendant's house.[95] From the Court's perspective, the method of surveillance was sufficiently invasive to raise Fourth Amendment protection because the information obtained could not have been acquired "without physical 'intrusion into a constitutionally protected area.'"[96] The Court noted the long history of Fourth Amendment protection for activity within the home, concluding that "the Fourth Amendment draws a firm line at the entrance to the house."[97] The statement regarding "a device that is not in general public use"[98] attempted to clarify that observations which could have been made through the use of well-known surveillance methods without a physical intrusion would not fall under the Fourth Amendment even if those observations revealed details about the home.[99] Basically, the lack of general awareness regarding the technology at issue strengthened the second prong of the *Katz* test—that the expectation of privacy is one society is prepared to recognize as reasonable.[100]

---

93. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (finding that electronic surveillance constitutes a search, and thus is presumptively unreasonable without a warrant, where "the Government uses a device that is not in general public use to explore details of the home that would previously have been unknowable without physical intrusion").

94. *Id.* at 40; *cf.* California v. Ciraolo, 476 U.S. 207, 215 (1986) (concluding that the Fourth Amendment does not protect an individual from observations, electronic or otherwise, that could have been made without a physical intrusion onto private property).

95. *Kyllo*, 533 U.S. at 29–30 (describing generally the manner in which thermal imagers are used and the way in which one was used in the instant case to detect the presence inside defendant's home of equipment used to grow marijuana).

96. *See id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

97. *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

98. *Id.*

99. *See Ciraolo*, 476 U.S. at 211 (positing that constructing a ten foot fence around one's property would be insufficient to protect a homeowner from observations made by law enforcement officers "perched on the top of a truck or a two-level bus").

100. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (emphasizing that in spite of advances in sense-enhancing technology there is still a "minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*" which must be protected "at least where . . . the technology in question is not in general public use").

After tracing the *Katz* line of cases, the *Kyllo* Court noted that determining what methods of surveillance were sufficiently known to the public such that an individual could not reasonably expect privacy from such surveillance requires a continual reevaluation of advances in technology.[101] Incorporating this new test for the propriety of electronic searches, for the purposes of CSLI disclosure, the general question is: Does this method of electronic surveillance reveal information that the target expects to remain private and is that expectation of privacy reasonable?[102] In order to answer this question it is necessary to consider whether the surveillance method obtains information that could not have been gathered by standard visual surveillance[103] as well as whether the technology at issue is in general public use.[104]

2. Assumption of Risk

From the perspective of CSLI disclosure cases, the right articulated in *Kyllo* to be free from surveillance not known to the general public is one of several factors that must be considered, along with the assumption of risk principle described in *United States v. Miller*.[105] The *Miller* Court addressed a government request for disclosure of financial records provided by customers to banking institutions.[106] Reasoning that the customers

---

101. *Id.* at 34 (presenting as an example "the technology enabling human flight [that] has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house . . . that once were private").

102. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

103. *See* United States v. Knotts, 460 U.S. 276, 285 (holding that the defendant had no "legitimate expectation of privacy" unless the surveilled activity "would not have been visible to the naked eye").

104. *See Kyllo*, 533 U.S. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

105. *See* United States v. Miller, 425 U.S. 435, 443–44 (1976) (concluding that individuals possess no reasonable expectation of privacy in information they voluntarily supply to banks because they assume the risk "that [such] information will be conveyed by [banks] to the Government").

106. *See id.* at 437–38 (responding to the Government's request for "all records of accounts, *i.e.*, savings, checking, loan or otherwise in the name of . . . [respondent]" without

assumed the risk that those records would be made available to the government when they voluntarily supplied them to the banks, the Court concluded that, absent a legitimate expectation of privacy, there was no Fourth Amendment search and thus no violation of the respondent's Fourth Amendment interest.[107]

In *Smith v. Maryland*,[108] the Court extended the *Miller* rationale to permit the installation of a pen register to record the numbers dialed on a targeted telephone.[109] The Court focused on the telephone user's knowledge that the numbers entered will be transmitted to the phone company.[110] Referencing the similar circumstances in *Miller*, the Court concluded that it had "consistently . . . held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[111] By using his phone, the party subject to pen register surveillance in that case was found to have voluntarily supplied the numbers to the phone company and "assumed the risk that the company would reveal to police the numbers he dialed."[112] Where the targeted party assumes the risk by voluntarily supplying information to third parties, the use of devices such as pen registers to collect this information does not constitute a search for Fourth Amendment purposes.[113]

Thus, information that would otherwise be protected by the Fourth Amendment can nonetheless be disclosed to the government absent a

---

informing the respondent that such disclosure was taking place (internal quotations omitted)).

107. *See id.* at 445 ("We hold that the District Court correctly denied respondent's motion to suppress, since he possessed no Fourth Amendment interest that could be vindicated by a challenge to the subpoenas.").

108. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (concluding that because "petitioner . . . entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate'" and, "consequently, [recording the dialed numbers] was not a 'search,' and no warrant was required").

109. *See id.* 736–37 n.1 (describing the installation of a pen register which is "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released").

110. *See id.* at 743 ("Telephone 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.").

111. *Id.* at 743–44.

112. *Id.* at 744.

113. *See id.* at 745–46 ("The installation and use of a pen register . . . was not a 'search.'").

showing of probable cause when it has been voluntarily surrendered.[114] Assumption of risk is typically claimed by the government in CSLI disclosure order cases.[115] The asserted rationale is that a cellular phone user voluntarily turns over this information to the cellular provider, and therefore, the user can have no objective expectation of privacy regarding CSLI.[116]

3. Relevant Statutes

Disclosure of CSLI is statutorily controlled generally by the Electronic Communications Privacy Act of 1986 (ECPA),[117] which was an attempt by legislators to find a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[118] However, the practical effect of the statute has been to extend the authority of law enforcement agencies to monitor cellular communications.[119] The second and third titles of the ECPA, commonly referred to as the Stored Communications Act (SCA)[120] and the Pen Register Statute,[121] along with the later enacted Communications Assistance for Law Enforcement Act (CALEA),[122] serve as the basic statutory framework within which CSLI jurisprudence has developed.

---

114. *See id.* at 745 (declining to make the question of whether to apply the Fourth Amendment turn on the individual practice of the third party to whom information is disclosed and instead basing the absence of a Fourth Amendment claim on the fact that the defendant "voluntarily conveyed" the information).

115. *See, e.g.*, Texas 2005 Opinion, 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005) ("The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in cell site location data, analogizing such information to the telephone numbers found unprotected in *Smith v. Maryland*.").

116. *See id.* (same).

117. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2006).

118. S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

119. *See* Lockwood, *supra* note 5, at 312 n.20 (noting that the ECPA "extend[ed] the baseline regulatory scheme for 'wire' communications to 'electronic' communications as well" (citing Pub. L. No. 99-508, 100 Stat. 1848 (1986))).

120. Electronic Communications Privacy Act of 1986 § 201, 18 U.S.C. §§ 2701–11 (2006).

121. *Id.* § 301, 18 U.S.C. §§ 3121–27 (2006).

122. *See* Communications Assistance for Law Enforcement Act §§ 102–12, 47 U.S.C. §§ 1001–10 (2006) [hereinafter CALEA] (intending to strike a balance between law enforcement's use of increasingly revealing electronic surveillance techniques and personal privacy interests).

a. The Pen Register Statute

A pen register, as described in the context of *Smith v. Maryland*, records the numbers dialed on a targeted telephone line.[123] In *Smith*, the Court found that installation and use of a pen register was not a Fourth Amendment search.[124] Because the use of pen registers did not constitute a search, Congress enacted the Pen Register Statute, which also covers the use of trap and trace devices,[125] to regulate the use of these surveillance techniques.[126] Trap and trace devices work in the opposite direction as pen registers, recording the electronic impulses that allow the government to identify the device making a call to the targeted device.[127] To obtain a court order allowing the use of a pen register or trap and trace device under the Pen Register Statute, the government needs to show "that the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[128]

The Pen Register Statute is fairly antiquated in light of modern technology.[129] Despite its narrow scope, the statute is still relevant to the controversy over CSLI disclosure in light of the government's attempts to obtain CSLI through the combined authority of the Pen Register Statute, the SCA, and the CALEA under the so called "hybrid theory," detailed below.[130] Additionally, for purposes of placing CSLI within the hierarchy of electronic-surveillance techniques, the Pen Register Statute serves as the

---

123. *See* Smith v. Maryland, 442 U.S. 735, 735 n.1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").

124. *See id.* at 745–46 (concluding that "petitioner . . . entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate'" and, "consequently, [there] was not a 'search,' and no warrant was required").

125. *See* 18 U.S.C. § 3121(a) (2006) (providing a general prohibition on the installation and use of pen registers or trap and trace devices without a court order).

126. *See* WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, CRIMINAL PROCEDURE 314 (5th ed. 2009) (discussing the structure of the Pen Register Statute and explaining how it is "explained by its unique history" as a legislative reaction to *Smith v. Maryland*).

127. *See* Texas 2005 Opinion, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) ("A 'pen register' is a device that records the numbers dialed for outgoing calls made from the target phone. A trap and trace device captures the numbers of calls made to the target phone.").

128. 18 U.S.C. § 3123(a)(1).

129. *See* LAFAVE ET AL., *supra* note 126, at 314 ("Modern technologies make the terminology of the pen register statute quite antiquated.").

130. *See infra* Part III.A.3.d (describing the "hybrid theory" and the reasons courts have largely rejected it).

first watermark—the most permissive, purely legislative control over a form of electronic surveillance that does not constitute a Fourth Amendment search.[131]

b. The Stored Communications Act

The SCA regulates government access to stored user account information compiled by third parties in the ordinary course of business.[132] CSLI is sought by the government as a "record or other information pertaining to a subscriber to or customer of such service" under 18 U.S.C. § 2703(c)(1).[133] CSLI disclosure cases are determined in large part by the reviewing court's willingness to apply § 2703(d) which provides:

> A court order for disclosure under subsection (b) or (c) . . . shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material to an ongoing criminal investigation*.[134]

While this section clearly defines the showing required to obtain information under it, whether CSLI can be obtained by presenting "specific and articulable facts" that the sought information is "relevant and material to an ongoing criminal investigation" is the crux of the current debate over CSLI.[135] Under the SCA, the contents of communications are subject to

---

131. *See* Texas 2010 Opinion, 727 F. Supp. 2d 571, 572–73 (W.D. Tex. 2010) (outlining the four types of electronic surveillance that federal permits to be used as "criminal investigative tools" and noting that pen registers and trap and trace devices are "in most contexts the least invasive tools").

132. *See* 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, 1212–23 (2004) (summarizing the goal of the SCA, the entities regulated by it, and the various disclosure requirements under its subsections, particularly as they relate to modern data collection techniques by internet service providers).

133. *See, e.g.*, Third Circuit Opinion, 620 F.3d 304, 306 (3d Cir. 2010) (noting that in the instant CSLI disclosure case "the Government seeks what is referred to as 'a record or other information pertaining to a subscriber to or customer of such service'").

134. 18 U.S.C. § 2703(d) (2006) (emphasis added).

135. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 586 (W.D. Pa. 2008) ("The Court emphasizes that the issue is not *whether* the Government can obtain movement/location information, but *only the standard* it must meet to obtain a Court Order for such disclosure and the basis of authority."), *vacated*, 620 F.3d 304 (3d Cir. 2010).

wholly different disclosure standards than subscriber records and other non-content information.[136] CSLI arguably falls into the non-content category of "record[s] or other information pertaining to a subscriber to or customer of such service."[137]

Because of this classification, the government has consistently argued that the SCA allows the disclosure of CSLI based on the satisfaction of § 2703(d)'s requirements.[138] Courts, however, have been reticent to permit disclosure under this standard because of both the obligation to protect individual privacy[139] and the express language in the SCA defining "electronic communications" to exclude "any communication from a tracking device."[140] Essentially, the debate over whether § 2703(d) applies to CSLI within the context of the SCA is a matter of statutory interpretation: Authority supports the conclusion that CSLI generally falls within the definition of a "record or other information pertaining to a subscriber or customer,"[141] but if cellular phones producing CSLI function as "tracking" devices then the language of the SCA itself exempts that information from disclosure under § 2703(d), and arguably subjects it to a

---

136. *Compare* 18 U.S.C. § 2703(a)–(b) (providing the requirements the government must satisfy to compel disclosure of the contents of electronic communications held in electronic storage and remote computing services), *with id*. § 2703(c)(1) (providing the ways in which "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose the record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)").

137. *Id.* § 2703(c)(1); *see* Texas 2010 Opinion, 727 F. Supp. 2d 571, 574 (W.D. Tex. 2010) ("Most courts have assumed (with little or no discussion) that historical CSLI may be obtained under the SCA because it only amounts to stored records.").

138. *See Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 588 ("The Government has applied, under the Stored Communications Act . . . 18 U.S.C. § 2703, for an Order requiring a cellular service provider to disclose . . . [CSLI] . . . on the basis of its asserted relevance to an ongoing criminal investigation . . . .").

139. *See id.* at 586 (noting that the judiciary is "entrusted with the protection of the individual civil liberties, including rights of privacy and rights of free association . . . paramount to the maintenance of our democracy").

140. *See id.* at 589 ("[T]he SCA expressly sets movement/location information outside its scope by defining 'electronic communications' to exclude 'any communication from a tracking device . . . .'"); *see also* 18 U.S.C. § 3117 (defining "Mobile tracking devices" for the purposes of the Stored Communications Act).

141. *See Texas 2010 Opinion*, 727 F. Supp. 2d at 574 ("Most courts have assumed (with little or no discussion) that historical CSLI may be obtained under the SCA because it only amounts to stored records.").

higher standard of proof before the government can obtain the information.[142]

i. What Constitutes a Tracking Device?

Under the SCA a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object."[143] In general, federal law requires a showing of probable cause prior to obtaining a warrant to install a tracking device or perform a search.[144] CSLI may be particularly difficult to identify as a "tracking device" under the SCA because the definition itself does not state any degree of specificity required in regard to the location information, and CSLI data is variably accurate depending on several factors—particularly the number of towers within range of the cellular phone at a given time.[145] In spite of the importance many courts and commentators have placed on this distinction,[146] even if CSLI is classified as a "tracking device," and therefore is not subject to disclosure under the SCA, the Supreme Court has held that tracking devices may be used without a showing of probable cause in many circumstances.[147] Thus, although federal law provides a procedure

---

142. *See Smith ECPA Reform Testimony*, 111th Cong. 82–83 (2010) (written statement of Stephen W. Smith, United States Mag. J.) (explaining why he reasoned the SCA did not apply to CSLI and noting that "[o]ther magistrate judges soon began to weigh in with [opinions] of their own" and "[m]any agreed").

143. 18 U.S.C. § 3117(b).

144. *See* FED. R. CRIM. P. 41(d) ("[A] magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

145. *See supra* Part II (describing the basic technology involved in creating CSLI data). *Compare* Lockwood, *supra* note 5, at 309 (recognizing that in rural areas "the location information available to providers is significantly less accurate simply because fewer towers are available" to receive a given phone's signal), *with id.* (explaining that in urban areas with multiple towers and where the towers are sectioned "into directional 'faces' (north face, south face, etc.)" and the significant number of towers in a relatively small area "gives providers access to quite accurate location information").

146. *See* Texas 2005 Opinion, 396 F. Supp. 2d 747, 753–57 (S.D. Tex. 2005) (engaging in a detailed analysis of "Prospective Cell Site Data as Tracking Information" after stating that "[o]ur analysis begins with the tracking device category").

147. *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding installation of an electronic tracking device implicated no Fourth Amendment concerns when that device was used to track their vehicles on public highways where they had no reasonable expectation of privacy), *with* United States v. Karo, 468 U.S. 705, 717 (1984) (rejecting the Government's claim that it should be able to use tracking devices to identify an object's

for the installation and use of tracking devices, if CSLI surveillance does not constitute a Fourth Amendment search, then failure to follow federal procedure or state regulations on law enforcement use of CSLI does not make out a constitutional violation. The only redress under federal law for a target who has been tracked by a device that was not installed pursuant to a warrant supported by probable cause is to move for suppression of that evidence.[148] While Rule 41 lays out the myriad of requirements for issuing a warrant for a tracking device,[149] absent infringement of a constitutional right, the target will be unable to suppress the location information obtained from that device.

c. The Communications Assistance for Law Enforcement Act

Enacted in 1994, the CALEA is the most recent federal statute directly concerning CSLI.[150] Congress's stated objective in passing the CALEA was to "protect privacy in the face of increasingly powerful and personally revealing technologies."[151] The legislation obligates telecommunications carriers to be able to provide call-identifying information to law enforcement.[152] Under the CALEA, "call-identifying information" is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any . . . telecommunications carrier."[153] The CALEA definition of call-identifying information contains a specific exception that is particularly relevant to CSLI disclosure:

---

location within a private residence absent a showing of probable cause).

148. *See* FED. R. CRIM. P. 41(h) (providing no remedy for violation of the statute other than allowing that "[a] defendant may move to suppress evidence in the court where the trial will occur").

149. *See id.* 41(e)(2)(C) (detailing the requirements for a warrant to install a tracking device).

150. Communications Assistance for Law Enforcement Act §§ 102–12, 47 U.S.C. §§ 1001–10 (2006).

151. H.R. REP. NO. 103-827, at 13 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3493.

152. *See* 47 U.S.C. § 1002(a) (2006) (requiring "telecommunications carrier[s] [to] ensure that [their] equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications" are capable of performing the functions described in the subsections of § 1002).

153. *Id.* § 1001(2).

"[S]uch call-identifying information shall not include any information that may disclose the physical location of the subscriber."[154]

Significant debate has arisen over whether CSLI is prohibited from disclosure by this provision of the CALEA.[155] Prior to the statute's passage, Louis Freeh, former director of the FBI, testified before Congress regarding the ways in which law enforcement was likely to use the provisions of the CALEA.[156] Freeh expressly disclaimed any intent to expand the authority of the government to obtain information via electronic surveillance.[157] However, in *Third Circuit Opinion*, the court reasoned that "the protections that Congress adopted for CSLI in 47 U.S.C. § 1002(a)(2) have no apparent relevance to § 2703(d)."[158] The CALEA was initially used in the CSLI context to justify disclosure under the now-disfavored hybrid theory.[159] The statute remains important not because it specifically permits or forbids disclosure of CSLI under the SCA, but because its legislative history speaks strongly to Congress's intent to prevent expansion of the location information that can be obtained by tracking electronic communications.[160]

i. The "Hybrid Theory"

---

154. *Id.* § 1002(a)(2)(B).

155. *See* Third Circuit Opinion, 620 F.3d 304, 314–15 (3d Cir. 2010) (disagreeing with the lower court's determination that the legislative history of the CALEA indicates a warrant should be required in order to obtain CSLI).

156. *See Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and Law of the S. Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the H. Judiciary Comm.*, 103d Cong. 5–46 (1994) (testimony and statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter *CALEA Joint Hearings*] (containing Director Freeh's response to Congress's questions, his prepared statement, and answers to specific interrogatories regarding the CALEA).

157. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 596 (W.D. Pa. 2008) (characterizing Freeh's testimony as "reassur[ing] Congress that law enforcement was not attempting to obtain via the 1994 enactments, or to otherwise alter the standards applicable to, movement/location information"), *vacated*, 620 F.3d 304 (3d Cir. 2010).

158. *Third Circuit Opinion*, 620 F.3d at 315.

159. *See infra* Part III.A.3.i (describing the "hybrid theory" and the reasons courts have largely rejected it).

160. *See CALEA Joint Hearings*, 103d Cong. 28 (1994) (testimony and statement of Louis J. Freeh, Director, Federal Bureau of Investigations) (telling Congress that the CALEA would "ensure[] the maintenance of the status quo" in regard to location information).

Government requests for CSLI have almost always included an argument that disclosure is permitted under the so-called hybrid theory.[161] Some courts found that although the SCA did not provide sufficient authority to obtain CSLI without probable cause in and of itself, the combined authority granted to the government by the SCA, CALEA, and the Pen Register Statute did allow CSLI to be obtained without showing probable cause.[162] The statutory argument claimed that the Pen Register Statute permits the capture of numbers for incoming and outgoing calls, and that when used on cellular phones these devices would also disclose CSLI at the beginning and end of each call.[163] Next, the government cited CALEA as requiring "that courts rely also on some additional statutory authority when ordering the disclosure of prospective cell site information under the Pen Register Statute," and contended that this additional authority was provided by the SCA.[164]

The first flaw in the hybrid theory is that the SCA contains specific restrictions on certain types of information disclosure, namely, prospective information, and although it also contains exceptions to this restriction, neither pen registers nor any other device covered by the Pen Register Statute are listed among those exceptions.[165] Furthermore, because the legislative history of CALEA indicates it was not intended to expand the

---

161. *See, e.g.*, Texas 2005 Opinion, 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005) (describing the Government's "hybrid theory," which combines parts of the PRS, the CALEA, and the SCA to argue for disclosure of CSLI at the SCA's "specific and articulable facts" standard).

162. *See In re* Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006) [hereinafter New York Oct. 2006 Opinion] (concluding "that [the court] can order the disclosure of prospective cell site information pursuant to the combined authority of the Pen Register Statute and the Stored Communications Act").

163. *In re* the Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Info., 497 F. Supp. 2d 301, 304–06 (D.P.R. 2007) [hereinafter Puerto Rico 2007 Opinion] (summarizing the "hybrid theory" argument both in the particular case and by referencing aspects of it that the government has used in other instances).

164. *See id.* at 305 (specifying the government's three part argument for disclosure under the "hybrid theory" (quoting *New York Oct. 2006 Opinion*, 460 F. Supp. 2d at 454)).

165. *See In re* the Application of the U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [Sealed] and [Sealed], 416 F. Supp. 2d 390, 395 n.7 (D. Md. 2006) [hereinafter Maryland 2006 Opinion] ("SCA regulates access to records and communications in storage and therefore lacks provisions typical of prospective surveillance statutes.").

ability of law enforcement to obtain location information,[166] using it as the linchpin of expanded surveillance under the SCA and the Pen Register Statute is widely seen as an implausible argument.[167] Due to numerous flaws that courts have found with the hybrid theory, this approach largely has fallen out of favor.[168]

4. "Probable Cause" Versus "Relevant and Material"

The difference between "probable cause" warrants and the standard required for information disclosure under 18 U.S.C. § 2703(d) provides substantially different protection for the targets of CSLI requests.[169] Probable cause requires law enforcement seeking the authority to perform a search or seizure to demonstrate facts that are "sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has or is being committed."[170] On the other hand, court orders issued under the "relevant and material" standard can target individuals who are not in any way suspected of criminal activity and gives access to evidence without

---

166. *See supra* Part III.A.3.c (describing the CALEA's legislative history and noting that during Congressional testimony a high ranking law enforcement official "expressly disclaimed any intent to expand the authority of the government to obtain information via electronic surveillance").

167. *See* Texas 2005 Opinion, 396 F. Supp. 2d 747, 764 (S.D. Tex. 2005) ("Far from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the Pen/Trap Statute has 'nothing to do with' the SCA, and that transactional information 'is exclusively dealt with in chapter 121 of Title 18,' *i.e.*, the SCA." (quoting *CALEA Joint Hearings*, 103d Cong. 27–28 (1994) (testimony and statement of Louis J. Freeh, Director, Federal Bureau of Investigations)).

168. *See* Texas 2010 Opinion, 727 F. Supp. 2d 571, 575 (W.D. Tex. 2010) (declining to even consider the hybrid theory because "[n]umerous cases have already exhaustively reviewed the Government's hybrid argument, and there is no need to restate the various failings courts have found with it").

169. *Compare* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (defining probable cause to exist where "the facts and circumstances within [the officers'] knowledge and of which they [have] reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has or is being committed"), *with* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 588 (W.D. Pa. 2008) (denying the government's request for CSLI regarding an individual not suspected of criminal activity but who purportedly associates with a "Criminal Suspect" on a showing of "specific and articulable facts" under 18 U.S.C. § 2703(d) (internal quotations omitted)), *vacated*, 620 F.3d 304 (3d Cir. 2010).

170. *Brinegar*, 338 U.S. at 175–76.

requiring any particularity that a crime has been or is being committed.[171] Compared to probable cause, disclosure under the relevant and material standard is both lower in the quantum of evidence required and broader in the individuals it can potentially target, particularly third parties.[172]

B. Competing Interpretations of the Law

Lacking a clear standard to apply, district courts have reached conflicting conclusions regarding CSLI disclosure cases, and these decisions have been based on a number of the rationales previously discussed.[173] Though not binding precedent, these decisions illustrate the various theories that inform CSLI disclosure cases, and their holdings provide background for analyzing the first U.S. Court of Appeals decision on the issue.[174]

Focusing on Congress's intent, the court in *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*[175] (*Texas*

---

171. *See Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 588 n.11 (describing the Government's application for CSLI disclosure as based on an assertion "that the Subscriber's cell phone is 'being used by' the Criminal Suspect" and "provid[ing] no specific information connecting these two individuals, or connecting the Criminal Suspect to the cell phone").

172. *See* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."); *id*. ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause *particularized with respect to that person*." (emphasis added)).

173. *See, e.g.*, New York Feb. 2006 Opinion, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) (accepting, in dicta, the Government's interpretation of SCA as authorizing it to obtain historical CSLI); Wisconsin Opinion, 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006) (concluding, in dicta and without analysis, that request for prospective CSLI requires probable cause because it requested prospective rather than historical information); New York Oct. 2005 Opinion, 396 F. Supp. 2d 294, 303 n.6 (E.D.N.Y. 2005) (stating, in dicta and without explanation, that "§ 2703(d) plainly allows" the Government to seek historical CSLI); Texas 2005 Opinion, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) (stating, in dicta, that were the communication service providers to compile the tracking information themselves, it would bring the information "more comfortably" within the scope of the Stored Communications Act).

174. *See* Third Circuit Opinion, 620 F.3d 304, 305–06 (3d Cir. 2010) ("This appeal gives us our first opportunity to review whether a court can deny a Government application under . . . § 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.").

175. *See Texas 2005 Opinion*, 396 F. Supp. 2d at 765 (concluding that absent clear Congressional intent, the reading of the statutes that avoids the Fourth Amendment question

2005 Opinion), preferred the probable-cause-required reading of the statute because it avoided the potential for a Fourth Amendment conflict.[176] Drawing on this analysis and further concentrating on broad issues raised by the private nature of location information, the court in *Pennsylvania 2008 Opinion* concluded probable cause was required for both historical and prospective CSLI.[177]

Alternatively, the Kansas district court specifically found probable cause was not required when the government used CSLI to confirm an individual's location on a public highway in real time.[178] This opinion extends the principle articulated in *Knotts* that surveillance that could lawfully be conducted in person implicates no Fourth Amendment concerns because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[179]

In another very specific holding, the Southern District Court of New York found probable cause is not required so long as the government's request is restricted to only that information regarding the tower receiving the transmission, the information is collected in relation to a call made or received by the cell phone user, and that information is provided to the government by the provider.[180] Because historical CSLI "only amounts to stored records," some courts have drawn a distinction between location

---

by requiring probable cause is preferable).

176. *See id.* (same).

177. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 615–16 (W.D. Pa. 2008) ("[M]ovement/location information . . . is the subject of express Congressional protection. Indeed, Congress has reiterated throughout the legislative history of its electronic communications legislation, and reflected in the provisions of its enactments, its recognition of an individual expectation of privacy in 'location information.'"), *vacated*, 620 F.3d 304 (3d Cir. 2010).

178. *See* United States v. Redd, No. 09-10099-JTM, 2010 U.S. Dist. LEXIS 103385, at *13 (D. Kan. Sep. 29, 2010) (finding that the use of CSLI to locate defendant in areas where visual surveillance could also be used did not require probable cause because "defendant had no reasonable expectation of privacy as he moved in plain view on public highways").

179. *Compare id.* ("[D]efendant had no reasonable expectation of privacy as he moved in plain view on public highways."), *with* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

180. *See In re* Application of U.S. for an Order for Disclosure of Telecomms. Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005) (holding that the specific information disclosed in that case did not require a showing of probable cause but retaining the option of finding such a requirement under future factual circumstances).

information used to track the target in real time and past location information, with "[m]ost courts [assuming] (with little or no discussion) that historical CSLI may be obtained under the SCA because it only amounts to stored records."[181] This line-drawing reflects privacy advocates' concern that prospective CSLI is inherently more invasive than historical CSLI.[182]

These decisions, all of which were published in the past seven years,[183] have not produced a dominant line of reasoning.[184] The Third Circuit was the first U.S. Court of Appeals to consider the issue, and its decision serves as the most significant analysis in this area to date.[185]

IV. Third Circuit Opinion

The court in *Third Circuit Opinion* concluded that "the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d)."[186] However, the court found that the SCA "as presently written gives the [reviewing judge] *the option* to require a warrant showing probable cause."[187]

---

181. Texas 2010 Opinion, 727 F. Supp. 2d 571, 574 (W.D. Tex. 2010).

182. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?* 29 HASTINGS COMM. & ENT. L.J. 421, 432 (2007) (arguing the inherent limitations on historical CSLI make it less troublesome from a personal privacy perspective).

183. *See Texas 2010 Opinion*, 727 F. Supp. 2d at 573–74 (outlining the series of cases "[b]eginning in 2005" that "address[ed] many of the questions raised by applications for CSLI").

184. *See* Third Circuit Opinion, 620 F.3d 304, 305–06 (3d Cir. 2010) (addressing the question of whether a court can deny the Government's application for CSLI disclosure once it has satisfied § 2703(d)'s burden of proof); *Texas 2010 Opinion*, 727 F. Supp. 2d at 573–74 (recognizing that while "[t]he majority approach . . . has been to require the same 'probable cause' showing for CSLI regardless of the means by which the information is acquired . . . a minority of decisions have allowed limited CSLI with only a showing of 'specific and articulable facts'"); *see also Smith ECPA Reform Testimony*, 111th Cong. 85 (2010) (written statement of Stephen W. Smith, United States Mag. J.) (pointing to "two systemic flaws in the existing statutory scheme" governing CSLI disclosure that merit reform).

185. *See Third Circuit Opinion*, 620 F.3d at 305–06 (considering "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").

186. *Id.* at 315.

187. *Id.* at 319 (emphasis added).

A. Background

The court began by laying out the brief facts relevant to the case before it, specifying that the government had "applied for a court order pursuant to . . . § 2703(d), to compel an unnamed cell phone provider to produce a customer's 'historical cellular tower data,' also known as cell site location information or 'CSLI.'"[188] After identifying generally the relevant portions of the SCA and CALEA,[189] Sections 2703(a) and 2703(b) were mentioned specifically in order to emphasize that the government's request was not for the contents of any communication.[190] The request was limited to "subscriber information" contained in § 2703(c).[191] Adopting the government's position, the court stated that "there is no dispute that historical CSLI is a 'record or other information pertaining to a subscriber . . . or customer,' and therefore falls within the scope of § 2703(c)(1)."[192] The court specified that the standard for disclosure of this data under § 2703(d) was a showing of "specific and articulable facts establishing reasonable grounds" that the information sought is "relevant and material to an ongoing criminal investigation."[193]

B. Is Probable Cause Required?

The court summarized Judge Lenihan's basic holding in the lower court, that "as a matter of statutory interpretation . . . nothing in the provisions of the electronic communications legislation authorizes it [i.e.,

---

188. *Id.* at 305.

189. *See id.* at 306 (identifying the SCA and CALEA as the statutes enacted after "[t]he growth of electronic communications . . . stimulated Congress to enact statutes that provide both access to information heretofore unavailable for law enforcement purposes and . . . protect users of such communication services from intrusion that Congress deems unwarranted").

190. *See id.* (specifying the scope of § 2703(a)'s coverage as "the *contents* of wire or electronic communications in electronic storage" and 2703(b)'s coverage as "the *contents* of wire or electronic communications held by a remote computing service" and noting that "[n]either of those sections is at issue here").

191. *See id.* ("The Government does not here seek disclosure of the contents of wire or electronic communications. Instead the Government seeks . . . 'a record or other information pertaining to a subscriber to or customer of such service' . . . ." (citing 18 U.S.C. § 2703(c)(1) (2006))).

192. *Id.* at 307–08.

193. *Id.* at 308.

the Magistrate Judge (MJ)] to order a [provider's] covert disclosure of CSLI absent a showing of probable cause under Rule 41."[194] Therefore, the first issue reviewed was whether the relevant and material disclosure standard adopted by the Government, or probable cause as proposed by the amici and adopted by the lower court, was required for obtaining the disclosure order.[195]

Looking at the language of the SCA and the MJ's rationale, the court noted that "[i]f CSLI could be characterized as information from a tracking device, and a tracking device is not covered by the SCA, this would be a relatively straightforward case because the Government, when seeking judicial permission to install or use a tracking device, must ordinarily obtain a warrant."[196] The court characterized the Government's CSLI request as consisting "of records of information collected by cell towers when a subscriber makes a cellular phone call."[197] The court recognized that "the record of a cell phone call does indicate generally where a cell phone was used when a call was made."[198] However, because the court determined that CSLI was a "wire communication," not an "electronic communication," even if a cell phone is deemed a tracking device, CSLI was not excluded by the SCA's disclosure provision prohibiting inclusion of "electronic communications" obtained from a tracking device.[199]

Next, the court addressed the lower court's determination that "even if the CSLI here is included within the scope of § 2703(c)(1), the Government must show probable cause because a cell phone acts like a tracking device."[200] The court indicated some reticence to permit disclosure of highly particular location information absent probable cause,[201] but distinguished the present case by characterizing historical CSLI as

---

194. *Id.*

195. *See id.* ("Thus, the counterpoised standards are 'probable cause,' the standard for a Rule 41 warrant, and the 'relevant and material' language in 18 U.S.C. § 2703(d).").

196. *Id.* at 309.

197. *Id.* at 310.

198. *Id.*

199. *See id.* at 309–10 ("[E]ven if the record of a cell phone call does indicate generally where a cell phone was used . . . 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.'").

200. *Id.* at 310–11.

201. *See id.* at 311 (recognizing that GPS technology can provide "much more precise location information" and expressly "tak[ing] no position whether a request for GPS data is appropriate under a § 2703(d) order").

"information tending to show that the cell phone user is generally at home from 7 p.m. until 7 a.m. the next morning (because the user regularly made telephone calls from that number during that time period)."[202] Rather than determine whether Judge Lenihan was right to conclude that probable cause was broadly necessary to protect citizens' legitimate expectations of privacy,[203] the court instead "consider[ed] whether there was any basis for the MJ's underlying premises"[204] that CSLI was protected by the Fourth Amendment and therefore a showing of probable cause is necessary in order to obtain it.[205] After analyzing the rationale behind *Knotts* and *Karo*,[206] the court found that these "opinions make clear that the privacy interests at issue are confined to the interior of the home."[207] The court concluded this first point by stating that: "We therefore cannot accept the MJ's conclusion that CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production."[208]

In summary, looking to Congress's intent, the court concluded that the standard for disclosure under § 2703(d) was meant to be lower than the probable cause required for tracking devices because "cell site information provides only a rough indication of a user's location at the time a call was made or received."[209] Thus, the court held that CSLI could be obtained under § 2703(d) and that probable cause need not be shown to require the disclosure.[210]

---

202. *Id.*

203. *See id.* at 312 (declining to consider "the premise that CSLI can track a cell phone user to his or her location, [which led] the MJ to conclude that CSLI would encroach upon what the MJ believed were citizens' reasonable expectations of privacy regarding their physical movements and locations").

204. *Id.*

205. *See id*. (discussing the Supreme Court's opinions in *Knotts* and *Karo* to illustrate what type of movement/location tracking falls within the Fourth Amendment's protection).

206. *See id*. (distinguishing *Karo* from *Knotts* on the basis that the tracking device in *Karo* did not reveal information about the interior of a home, and therefore did not reveal location information protected by the Fourth Amendment).

207. *Id.*

208. *Id.* at 313.

209. *See id.* at 312; *see also id.* at 311–12 (discussing the competing interpretations of FBI Agent William Shute's testimony regarding the specificity of CSLI as a possible tracking device).

210. *See id.* at 313 ("In sum, we hold 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.").

C. Discussion of Legislative History

The Third Circuit disagreed with the lower court's determination that the "relevant legislative history indicates that Congress did not intend its electronic communications legislation to be read to require, on its authority, disclosure of an individual's location information."[211] The court points to numerous statements in the SCA's legislative history that indicate the act was intended to serve two purposes: Provide protection for private citizens from increasingly invasive electronic surveillance and, at the same time, make that technology available to the government for law enforcement purposes.[212] Based on this language and Congress's stated aim in amending the statute through the CALEA "to keep pace with technological changes,"[213] the court concluded that "[t]he legislative history strongly supports the conclusion that the present standard in § 2703(d) is an 'intermediate' one" below probable cause.[214]

The court also disputed Judge Lenihan's interpretation of FBI Director Louis Freeh's testimony.[215] Judge Lenihan had concluded that "Director Freeh reassured Congress that law enforcement was not attempting to obtain via the 1994 enactments, or to otherwise alter the standards applicable to, movement/location information."[216] Because Director Freeh's testimony had been focused on obtaining tracking information from a pen register or trap and trace device, and use of those devices is governed by a standard lower than that required for disclosure under § 2703(d), the

---

211. Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 610 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010); *see* Third Circuit Opinion, 620 F.3d 304, 313 (3d Cir. 2010) ("We also have reviewed the legislative history of the SCA and find no support for [the magistrate judge's] conclusion.").

212. *See Third Circuit Opinion*, 620 F.3d at 313 (citing Senate and House reports to the effect that the legislation was intended to "protect[] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs" (quoting S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555)).

213. *Id.* at 314.

214. *See id.* ("Senate Report No. 103-402 states that § 2703(d) 'imposes an intermediate standard to protect on-line transactional records.'" (quoting S. Rep. No. 103-402, at 10 (1994))).

215. *See id.* ("Director Freeh's testimony, referred to by the MJ, does not provide support for the MJ's conclusion that a warrant is required to obtain CSLI.").

216. *Pennsylvania 2008 Opinion*, 534 F. Supp. 2d at 596.

court found that the testimony was not probative of Congress's intent with regard to § 2703(d)'s relevant and material standard.[217]

D. Can Probable Cause Ever Be Required?

The court then proceeded to consider whether magistrate judges have the discretion to require a probable cause warrant on a case-by-case basis.[218] The court considered the amici's argument[219] that the statute's language established a necessary, but insufficient, condition for disclosure of the requested information.[220] The court agreed with the government that "a magistrate judge does not have arbitrary discretion"[221] to require probable cause in a given case,[222] but expressed concern "with the breadth of the Government's interpretation of the statute that could give the Government the virtually unreviewable authority to demand a § 2703(d) order on nothing more than its assertion."[223] The court recognized that the government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home."[224]

In response to the Fourth Amendment concerns, the Government advanced the argument that CSLI was not protected because the subscriber

---

217. *See* Third Circuit Opinion, 620 F.3d 304, 314–15 (3d Cir. 2010) (discussing the focus of Director Freeh's testimony on pen register and trap and trace devices and concluding that "the legislative history does not show that Congress intended to exclude CSLI or other location information from § 2703(d)").

218. *See id.* at 315 (addressing the contention of the amici "that magistrate judges do have the discretion to require warrants").

219. *See id.* at 306 n.1 (explaining that "because the Government's application was *ex parte*, there was no adverse party to review or oppose it," but the court received amici briefs from the Electronic Frontier Foundation, the ACLU-Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology "hereafter jointly referred to as 'EFF'").

220. *See id.* at 316 (discussing the argument that the "only if" language in § 2703(d) should be read as a necessary condition for disclosure but that satisfaction is not sufficient in-and-of-itself to compel disclosure).

221. *Id.*

222. *See id.* ("Indeed, no judge in the federal courts has arbitrary discretion to issue an order.").

223. *Id.* at 317.

224. *Id.*

had voluntarily disclosed that information to a third party.[225] The Third Circuit considered the Government's assumption of risk argument,[226] and summarily rejected it.[227] The court agreed with the EFF that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."[228]

Lastly, the court revisited *Karo* in order to illustrate the importance of Fourth Amendment oversight.[229] The court lamented the "failure of Congress to make its intention clear"[230] and concluded that "[a] review of the statutory language suggests that the Government can proceed to obtain records pertaining to a subscriber by several routes, one being a warrant with its underlying requirement of probable cause, and the second being an order under § 2703(d)."[231] Based on this interpretation, the court found that, as written, the statute gave magistrate judges the option to require a showing of probable cause in any individual case, while recommending that this option be used sparingly.[232] Applying these principles to the instant case, the court vacated the magistrate judge's order denying the Government's application, and remanded the application to the district court to determine whether the Government had satisfied the standard of specific and articulable facts that are relevant and material.[233]

---

225. *See id.* ("The Government argues that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider.").

226. *See id.* (discussing the Government's citation to *United States v. Miller* and *Smith v. Maryland*).

227. *See id.* ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

228. *Id.*

229. *See id.* at 318 (looking to the Supreme Court's decision in *Karo* for the general proposition that "[i]ndiscriminate 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" (quoting United States v. Karo, 468 U.S. 705, 716 (1984))); *see also id.* ("The Government is also not free from the warrant requirement merely because it is investigating criminal activity.").

230. *Id.* at 319.

231. *Id.*

232. *See id.* (conceding that "the statute as presently written gives the MJ the option to require a warrant showing probable cause" but recommending that "it is an option to be used sparingly because Congress also included the option of a § 2703(d) order").

233. *See id.* (noting that MJ never determined whether the government actually made the showing required by § 2703(d) and remanding for determination of that issue).

E. Judge Tashima's Concurrence

Judge Tashima concurred with the majority in *Third Circuit Opinion*, and wrote separately to address concerns regarding the level of discretion that the court appeared to be granting to magistrate judges.[234] Judge Tashima was in agreement with the majority that § 2703(d) articulates the burden of proof the government must show to compel CSLI disclosure,[235] but disagreed with the proposition that magistrate judges retained the discretion to require a showing of probable cause in individual cases.[236]

In response to these concerns, the concurrence proposes that a magistrate judge should only be able to deny a disclosure request if the magistrate judge: (1) "finds that the government failed to present specific and articulable facts sufficient to meet the standard under § 2703(d)"; or (2) "finds that the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of the home."[237]

V. Analysis of Third Circuit Opinion

The Third Circuit's opinion arrives at a strange conclusion: Magistrate judges are granted discretion to require a showing of probable cause in individual cases, but this discretion is to be used sparingly, and no specific guidance is provided as to when this discretionary action is warranted.[238] Judge Tashima's concurrence recognizes this incongruity and provides a coherent recommendation for when such discretion should be exercised.[239]

---

234. *See id.* at 319 (Tashima, J., concurring) ("I write separately, however, because I find the majority's interpretation of the discretion granted to a magistrate judge by 18 U.S.C. § 2703(d) troubling.").

235. *See id.* at 319–20 (agreeing with the majority's holding 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").

236. *See id.* at 320 (claiming that "the majority then appears to contradict its own holding" by stating that "the statute as presently written gives the MJ the option to require a warrant showing probable cause").

237. *See id.* (citing Kyllo v. United States, 533 U.S. 27, 35–36 (2001)).

238. *See* Third Circuit Opinion, 620 F.3d 304, 319 (3d Cir. 2010) (concluding that the Stored Communications Act "as presently written gives the [reviewing judge] *the option* to require a warrant showing probable cause" (emphasis added)).

239. *See id.* at 320 (Tashima, J., concurring) (recommending that "the magistrate may

If CSLI reveals location information inside of a private residence, that information is protected by the Fourth Amendment.[240] The court is explicit throughout the opinion in recognizing the importance of protecting privacy in the home.[241] How then, does the court arrive at a conclusion that would generally permit the government to order disclosure of information that potentially was obtained from inside a private residence absent a probable cause requirement?

A. The Third Circuit's Interpretation of CSLI Technology

The answer to this question can be gleaned from a number of the court's statements regarding CSLI technology. In the court's discussion of whether CSLI should be classified as a wire communication or an electronic communication, CSLI is described as "records of information collected by cell towers when a subscriber makes a cellular phone call."[242] The conclusion that CSLI may in some instances be properly classified as information from a tracking device is thereafter predicated on circumstances where "the record of a cell phone call does indicate generally where a cell phone was used *when a call was made*."[243] Later, the court summarizes its impression of historical CSLI as possibly "provid[ing]

---

refuse to issue the § 2703(d) order" if "the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of the home").

240. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))); *Third Circuit Opinion*, 620 F.3d at 318 ("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." (quoting United States v. Karo, 468 U.S. 705, 716 (1984))).

241. *See Third Circuit Opinion*, 620 F.3d at 312 (looking to the Supreme Court's decisions in *Knotts* and *Karo* and concluding that those "opinions make clear that the privacy interests at issue are confined to the interior of the home"); *id.* at 317 (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home"); *id.* at 318 ("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." (quoting United States v. Karo, 468 U.S. 705, 716 (1984))).

242. *Id.* at 310.

243. *Id.* (emphasis added).

information tending to show that the cell phone user is generally at home from 7 p.m. until 7 a.m. the next morning (because the user regularly made telephone calls from that number during that time period)."[244] Clearly, the court is proceeding on the understanding that CSLI is only created when a user makes or receives a phone call. This is simply not the case. CSLI is created whenever a cellular phone registers with the network, a process that occurs approximately every seven seconds.[245] In the hands of law enforcement, disclosed CSLI can be used to provide detailed information about the location and movement of an individual carrying the device, even if that individual never makes a call.[246]

The fundamental misunderstanding about the breadth of information CSLI provides is also implicit in Judge Tashima's concurring opinion.[247] After recognizing that the discretion the majority granted to magistrate judges is arbitrary,[248] Judge Tashima proposes to "cabin the magistrate's discretion"[249] to require probable cause only where the government has failed to make the requisite showing under § 2703(d),[250] or where "it allows

---

244. *See id.* at 311 (concluding that "[w]ith that information, the Government may argue in a future case that a jury can infer that the cell phone user was at home at the time and date in question").

245. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) ("Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers serving their network and scanning for the one that provides the strongest signal/best reception. This process, called 'registration', occurs approximately every seven seconds."), *vacated*, 620 F.3d 304 (3d Cir. 2010); Lockwood, *supra* note 5, at 309 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

246. *See* Lockwood, *supra* note 5, at 312 ("The reality that people carry their cell phones on their persons means that cell phone tracking technology potentially offers a detailed view of a given subscriber's movements rather than simply providing call-identifying information."); *see also id*. at 309 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

247. *See* Third Circuit Opinion, 620 F.3d 304, 319–20 (3d Cir. 2010) (Tashima, J., concurring) (expressing disagreement with the majority opinion's grant of discretion to magistrate judges to require probable cause and advocating for a showing of probable cause only when the information will place the cell phone user within the home with no mention of how often this will occur).

248. *See id.* at 320 ("[T]he majority's interpretation of the statute . . . vests magistrate judges with arbitrary and uncabined discretion to grant or deny issuance of § 2703(d) orders at the whim of the magistrate . . . .").

249. *Id.*

250. *See id.* ("I would cabin the magistrate's discretion by holding that the magistrate may refuse to issue the § 2703(d) order only if she finds that the government failed to present specific and articulable facts sufficient to meet the standard under § 2703(d) . . . .").

police access to information which reveals a cell phone user's location within the interior or curtilage of the home."[251] Ironically, Tashima's recognition that granting magistrate judges the discretion to require probable cause is unwarranted unless the Fourth Amendment is implicated, which presumably would lead to most disclosure requests being granted based on satisfying § 2703(d),[252] actually illustrates why probable cause should almost always be required—CSLI provides sufficiently detailed information to implicate the Fourth Amendment in almost every case.[253]

B. What Is Protected by the Fourth Amendment?

Although the Third Circuit's opinion appears to mischaracterize CSLI technology,[254] the court is consistent throughout its opinion in identifying how integral the Fourth Amendment is to this issue.[255] The court explicitly rejects the argument that cell phone users voluntarily disclose their location information to third parties.[256] Additionally, there are numerous statements in the opinion expressing the court's concern that CSLI might be able to provide law enforcement information about an individual's location within

---

251. *Id.*

252. *See id*. ("[T]he magistrate may refuse to issue the § 2703(d) order here only if she finds that the government failed to present specific and articulable facts sufficient to meet the standard under § 2703(d) or, alternatively, finds that the order would violate the Fourth Amendment absent a showing of probable cause . . . .").

253. *See infra* Part VI (describing the extremely limited circumstances in which CSLI would not place targets within their homes).

254. *See supra* Part V.A (pointing out language in *Third Circuit Opinion* which indicates the court's misunderstanding that CSLI is only created when a call is made or received).

255. *See* Third Circuit Opinion, 620 F.3d 304, 312 (3d Cir. 2010) (looking to the Supreme Court's decisions in *Knotts* and *Karo* and concluding that those "opinions make clear that the privacy interests at issue are confined to the interior of the home"); *id.* at 317 (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home"); *id.* at 318 ("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." (quoting United States v. Karo, 468 U.S. 705, 716 (1984))); *id.* at 320 (Tashima, J., concurring) (proposing magistrate judges should only be permitted to exercise their discretion to require probable cause in cases where "the order would violate the Fourth Amendment absent a showing of probable cause").

256. *See id.* at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

a private residence.[257] The court also states that the general public is not aware of this passive electronic surveillance technology.[258] What the majority opinion glosses over is how a reviewing magistrate judge should take these interests into account in deciding whether or not to issue a disclosure order.[259] The concurrence by Judge Tashima posits the answer to this question by noting that where the magistrate judge expects the information sought will implicate the Fourth Amendment, probable cause should be required.[260] However, Judge Tashima seems to indicate that CSLI requests will rarely implicate the Fourth Amendment.

The court's grant of discretionary authority to magistrate judges is troublesome in two respects. First, if the Fourth Amendment does not protect CSLI, the statutory standard is clear and there is no articulable basis for demanding a showing of probable cause.[261] This recognition is reflected in the court's admonishment that though "the statute as presently written gives the MJ the option to require a warrant showing probable cause . . . it is an option to be used sparingly."[262] Second, if the Fourth Amendment does protect the location information sought, the probable cause requirement attaches. Although the legislative history may be ambiguous

---

257. *See id.* at 312 (looking to the Supreme Court's decisions in *Knotts* and *Karo* and concluding that those "opinions make clear that the privacy interests at issue are confined to the interior of the home"); *id.* at 317 (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home"); *id.* at 318 ("'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.'" (quoting United States v. Karo, 468 U.S. 705, 716 (1984))).

258. *See id.* at 317 (agreeing with the EFF that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information").

259. *See id.* at 319 (refusing to remove the option to require a warrant in an individual case and remanding only with instruction that the magistrate judge "give a full explanation that balances the Government's need . . . for the information with the privacy interests of cell phone users").

260. *See id.* at 320 (Tashima, J., concurring) (recommending the magistrate's discretion to require probable cause be exercised where "the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of the home").

261. *See id.* at 319 (majority opinion) ("A warrant requires probable cause, but there is no such explicit requirement for securing a § 2703(d) order.").

262. *See id.* (recommending the option to require probable cause be used sparingly after consistently noting that under § 2703(d) "there is no such explicit requirement").

with regard to whether Congress intended to permit disclosure of location information,[263] there is no indication that it intended to erode privacy in the home where an individual's Fourth Amendment interest is strongest.[264]

VI. Proposed Solution

Viewing the court's analysis in light of the realities of CSLI technology, the precedent it creates for lower courts is both inadequate to protect the residential privacy interests of individuals and gives unclear guidance to law enforcement seeking to use CSLI for legitimate purposes. However, there is a ready solution to this incongruity that can be extrapolated from the majority and concurring opinions.

First, the court repeatedly notes that if CSLI reveals location information about the interior of the home, that information raises Fourth Amendment concerns.[265] Judge Tashima's concurrence specifically cited disclosure of location-within-the-home information as the circumstance which should cause a magistrate judge to require a showing of probable cause.[266] On the other hand, CSLI that tracks an individual's location

---

263. *See supra* Part IV.C (discussing the Third Circuit's interpretation of the SCA's legislative history in comparison to the lower court's contrary interpretation).

264. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))); Third Circuit Opinion, 620 F.3d 304, 317 (3d Cir. 2010) (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home").

265. *See Third Circuit Opinion*, 620 F.3d at 312 (looking to the Supreme Court's Fourth Amendment decisions in *Knotts* and *Karo* and concluding that those "opinions make clear that the privacy interests at issue are confined to the interior of the home"); *id.* at 317 (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home"); *id.* at 318 ("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." (quoting United States v. Karo, 468 U.S. 705, 716 (1984))).

266. *See id.* at 320 (Tashima, J., concurring) (recommending the magistrate's discretion to require probable cause be exercised where "the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of the home").

outside of the home is indistinguishable from location information that could be obtained via in-person surveillance.[267] As the court makes clear and precedent amply supports, this type of public-location surveillance does not implicate the Fourth Amendment.[268] Thus, the threshold determination must be whether a given disclosure order will likely reveal an individual's location within the home.

In order to answer this question in the negative, a reviewing magistrate judge would have to decide that automatic cell phone registration, which takes place approximately every seven seconds,[269] would not place the target within the home at any point during the period for which disclosure is requested. Placement of an individual within their residence during the period of time for which CSLI is sought implicates the Fourth Amendment and its probable cause requirement.[270]

To see just how often this situation will arise, it may be illustrative to return to the hypothetical presented at the end of Part II.[271] Assume the government obtains a broad CSLI disclosure order on a Monday. Historical CSLI from a specific date prior to that Monday would implicate the Fourth Amendment if the target was within her home, with her cell phone on her

---

267. *See* United States v. Knotts, 460 U.S. 276, 281, 285 (1983) (finding the surveillance target's Fourth Amendment interest was not implicated where the surveillance "amounted principally to the following of an automobile on public streets and highways").

268. *See id.* at 281 (characterizing the government's permissible electronic surveillance in this case as "amount[ing] principally to the following of an automobile on public streets and highways"); *id.* at 285 (finding installation of an electronic tracking device implicated no Fourth Amendment concerns when that device was used to track their vehicles on public highways where they had no reasonable expectation of privacy); *Third Circuit Opinion*, 620 F.3d at 312 (looking to the Supreme Court's Fourth Amendment decisions in *Knotts* and *Karo* and concluding that those "opinions make clear that the privacy interests at issue are confined to the interior of the home").

269. *See* Pennsylvania 2008 Opinion, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) ("Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers serving their network and scanning for the one that provides the strongest signal/best reception. This process, called 'registration', occurs approximately every seven seconds."), *vacated*, 620 F.3d 304 (3d Cir. 2010).

270. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))); Third Circuit Opinion, 620 F.3d 304, 317 (3d Cir. 2010) (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home").

271. *See supra* Part II (identifying the differences between historical, prospective, and real-time CSLI through a hypothetical adapted from *Maryland 2005 Opinion*).

person, on that particular date. On Friday, when law enforcement returned to obtain CSLI from Wednesday and Thursday, that prospective CSLI is protected by the Fourth Amendment if the target was inside the home with her cell phone turned on during Wednesday or Thursday. Finally, when tracking the target's phone in real time, that real time CSLI invades the Fourth Amendment when the target enters her private residence.

Cell phones are a ubiquitous feature of modern life.[272] Cell phone users will have their phones on them just as surely as they will, at some point in time within the scope of a CSLI request, be located at home.[273] Therefore, because CSLI will almost always reveal information about the interior of the home that is protected by the Fourth Amendment, magistrate judges should either require a showing of probable cause, or allow law enforcement to only use CSLI that does not reveal information about the interior of the home.[274] Functionally, as Judge Tashima proposes, magistrate judges could "condition [their] order[s] by requiring minimization to exclude those portions which disclose location information protected by the Fourth Amendment, *i.e.*, within the home and its curtilage."[275]

Structuring disclosure requests in this manner would extend to the realm of electronic surveillance the principle that law enforcement can follow a suspect without probable cause in public, but not inside a private residence.[276] In circumstances where law enforcement legitimately needs location information that places the target within a private residence, as the Third Circuit noted, probable cause is typically not difficult to

---

272. *See* CTIA-The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey*, (2010) http://ctia.org/ (last visited Feb. 20, 2010) (estimating that as of June 2010 there were 292,847,098 cell phone in use in the United States and 251,618 cell sites) (on file with the Washington and Lee Law Review).

273. *See* Lockwood, *supra* note 5, at 312 ("The reality [is] that people carry their cell phones on their persons . . . .").

274. *See* Third Circuit Opinion, 620 F.3d 304, 319 (3d Cir. 2010) ("[I]t is imperative that the MJ make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users."); *id.* at 320 (Tashima, J., concurring) (recommending that the discretion to require a showing of probable cause be exercised if "the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of his home").

275. *Id.* at 320 n.10 (Tashima, J., concurring).

276. *See supra* Part III.A.1 and notes 81–92 (discussing the distinction the Supreme Court drew in *Knotts* and *Karo* between surveillance in public and within the home).

demonstrate.[277] This modest limitation: (1) recognizes that in light of modern technology the starting point for CSLI disclosure analysis must presuppose that a target's Fourth Amendment interest will be implicated; and (2) is consistent with the Supreme Court's prior Fourth Amendment jurisprudence.[278] However, although a general requirement of probable cause and a limitation on CSLI that invades the home would be seen as a victory for personal privacy in comparison to the Third Circuit's conclusion,[279] it is worth considering precisely what is left for the Fourth Amendment to protect.

VII. Conclusion

As CSLI has become an increasingly important tool for law enforcement, courts have struggled to find a balance that recognizes the statutory authorization for disclosure and at the same time acknowledges the personal privacy interests at stake.[280] While numerous courts and commentators have joined the call for Congress to reform and clarify the relevant legislation,[281] until that occurs, magistrate judges routinely face the very real task of ruling on disclosure orders with only the current statutory framework as a guide.

---

277. *Third Circuit Opinion*, 620 F.3d at 317 n.8 ("In our experience, magistrate judges have not been overly demanding in providing warrants as long as the Government is not intruding beyond constitutional boundaries.").

278. *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding installation of an electronic tracking device implicated no Fourth Amendment concerns when that device was used to track their vehicles on public highways where they had no reasonable expectation of privacy), *with* United States v. Karo, 468 U.S. 705, 717 (1984) (rejecting the Government's claim that it should be able to use tracking devices to identify an object's location within a private residence absent a showing of probable cause).

279. *See Third Circuit Opinion*, 620 F.3d at 319 (concluding that "the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d)").

280. *See supra* Part III.B (outlining the conflicting decisions and rationales of district courts in CSLI disclosure order cases).

281. *See* Third Circuit Opinion, 620 F.3d 304, 319 (3d Cir. 2010) (noting the difficulty facing courts addressing the proper standard to apply to CSLI disclosure orders and stating that "[t]he considerations for and against [a probable cause] requirement would be for Congress to balance"); *Smith ECPA Reform Testimony*, 111th Cong. 85–90 (2010) (written testimony of Hon. Stephen W. Smith, United States Mag. J.) (proposing Congress enact numerous reforms to the ECPA in light of the difficulty judges face in deciding disclosure order cases).

The Third Circuit attempted to provide guidance on this issue, but although much of its opinion accurately discussed the relevant constitutional considerations, a fundamental misunderstanding about CSLI technology led the court to conclude the Fourth Amendment would rarely be implicated,[282] in spite of the fact that where information about the interior of the home is at issue, the Fourth Amendment "draws a firm line."[283] Thus, in the case of CSLI, the starting point must be to recognize that information about the interior of the home will almost always bring Fourth Amendment considerations to the fore.

Future disclosure order cases should follow Judge Tashima's recommendation that a magistrate judge should only be able to deny a disclosure request if the magistrate judge: (1) "finds that the government failed to present specific and articulable facts sufficient to meet the standard under § 2703(d)"; or (2) "finds that the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of the home."[284] However, because the order will, in almost all cases, violate the Fourth Amendment absent a showing of probable cause, the magistrate judge should routinely "condition [the] order by requiring minimization to exclude those portions which disclose location information protected by the Fourth Amendment, *i.e.*, within the home and its curtilage."[285]

Finally, while the current state of Fourth Amendment jurisprudence advocates strongly for the solution this Note proposes, it is worth considering just what this state of affairs means for personal privacy. There are almost 300 million cellular phones being used in the United States.[286] These phones are in constant communication with over 250,000 cell sites

---

282. *See supra* Part V.A (illustrating the Third Circuit's misunderstanding that CSLI is only created when a cell phone makes or receives a call).

283. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))).

284. *See Third Circuit Opinion*, 620 F.3d at 320 (Tashima, J., concurring) (citing *Kyllo*, 533 U.S. at 35–36).

285. *Id.* at 320 n.10.

286. *See* CTIA-The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey*, (2010) http://ctia.org/ (last visited Feb. 20, 2010) (estimating that as of June 2010 there were 292,847,098 cell phone in use in the United States) (on file with the Washington and Lee Law Review).

that can be used to pinpoint an individual's location.[287] That these phones are almost always carried on an individual's person is almost too plain an observation to warrant stating.[288] Practically speaking, there are almost 300 million tracking devices being carried around in the United States, and at best the Constitution protects them from being used to track a target's location when that target enters his or her home.[289] The target may be tracked up until the moment the home is entered, and tracking may resume as soon as the target is once again beyond the home and its curtilage.[290] Is this really the type of surveillance the Court had in mind when it defined the limits on law enforcement use of tracking devices in *Knotts* and *Karo*?

Unfortunately, while courts have been struggling with CSLI disclosure order cases for some time,[291] Congress has only recently taken notice and reform legislation does not appear imminent.[292] As a judicial remedy, the compromise proposed by this Note draws a line that at least preserves Fourth Amendment protection where it has traditionally been deemed

---

287. *See id.* (estimating that as of June 2010 there were 251,618 cell sites in the United States).

288. *See* Lockwood, *supra* note 5, at 312 ("The reality [is] that people carry their cell phones on their persons . . . .").

289. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))); Third Circuit Opinion, 620 F.3d 304, 317 (3d Cir. 2010) (expressing concern that the Government's position would preclude magistrate judges from making particularized determinations as to whether the "disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home"). *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding installation of an electronic tracking device implicated no Fourth Amendment concerns when that device was used to track their vehicles on public highways where they had no reasonable expectation of privacy), *with* United States v. Karo, 468 U.S. 705, 717 (1984) (rejecting the Government's claim that it should be able to use tracking devices to identify an object's location within a private residence absent a showing of probable cause).

290. *See Third Circuit Opinion*, 620 F.3d at 320 (Tashima, J., concurring) (recognizing that CSLI location tracking only violates the Fourth Amendment when "it allows police access to information which reveals a cell phone user's location within the interior or curtilage of his home").

291. *See* Texas 2010 Opinion, 727 F. Supp. 2d 571, 573–74 (W.D. Tex. 2010) (outlining the series of cases "[b]eginning in 2005" that "address[ed] many of the questions raised by applications for CSLI").

292. *See Smith ECPA Reform Testimony*, 111th Cong. 79–91 (2010) (written testimony of Hon. Stephen W. Smith, United States Mag. J.) (informing Congress of the problems faced by magistrate judges reviewing CSLI disclosure requests and proposing numerous legislative solutions, none of which have been enacted in the ensuing months).

strongest,[293] but the limitations of that protection in comparison to the amount of tracking data the government can access without a showing of probable cause should give one pause. Until Congress takes action or the Court reconsiders its tracking device jurisprudence in light of modern technology, this is where the dispute will lie. The Fourth Amendment remains a bulwark against invasion of the home. But take just one step outside the castle and it is clear that the lines have been drawn in such a way that personal privacy, in terms of location information, is a thing of the past.

293. *See Kyllo*, 533 U.S. at 40 ("[T]he Fourth Amendment draws 'a firm line at the entrance to the house.'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))).