Washington and Lee Law Review

Volume 66 | Issue 4 Article 8

Fall 9-1-2009

Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard

Patrick T. Chamberlain

Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard

Patrick T. Chamberlain*

Table of Contents

* Candidate for J.D., Washington and Lee University School of Law, May 2010; B.A., University at Albany, State University of New York, 2006. I would like to thank the following individuals, for whose valuable guidance and feedback I am significantly indebted: Professor Erik Luna, Alexis Hawley, Mike McCarthy, and Bridget Tainer-Parkins. I would also like to thank my family for their support and my fiancée, Karen, for her unwavering care and patience throughout this process, including (most notably) her surprising willingness to put up with me.

I. Introduction

Although the inherent tension between technological development and individual privacy has long been a familiar source of legal conflict, the passage of time has intensified, rather than alleviated, this tension. Justice Brandeis, writing over eighty years ago in dissent in *Olmstead v. United States*,[1] correctly predicted the progressive exacerbation of this tension, noting his expectation that the continued growth of electronic surveillance ultimately would undermine the protection of individual privacy:

> "[T]ime works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[2]

Since then, this prediction has been vindicated—law enforcement agencies have continued to develop and take advantage of new technologies to assist their investigations, resulting in more intrusive invasions upon individual privacy.[3] One of the most prevalent modern incarnations of this phenomenon is the availability and use of cell site location information (CSLI).

---

1. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (finding no Fourth Amendment search in the government's installation of a wiretap device on the phone line outside of the defendant's residence because there was no physical trespass upon the defendant's property), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

2. *Id.* at 473 (Brandeis, J., dissenting).

3. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 29–30 (2001) (discussing police use of

CSLI derives from the process by which cellular phones communicate with nearby service towers.[4] This process occurs continuously while a phone is turned on[5] and without any action on the part of the phone's user.[6] From this process, cellular service providers (CSPs) receive details regarding the tower locations relied upon by users, which in turn can provide a relatively detailed picture of those users' geographic whereabouts.[7]

CSLI has an enormous investigative utility for law enforcement agencies.[8] Given the level of detail that such information contains, CSLI functionally provides the government with the ability to track suspects.[9] To capitalize on the availability of this potent tool, federal law enforcement officials more frequently have begun to seek court orders to compel CSPs to disclose particular users' CSLI.[10] Law enforcement applications for court orders in this

---

thermal imaging devices to detect amounts of heat within a residence); United States v. Knotts, 460 U.S. 276, 277 (1983) (describing tracking beepers as "radio transmitter[s] . . . which emit[] periodic signals that can be picked up by a radio receiver," thereby allowing the tracking of individuals and objects); Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (discussing law enforcement use of "pen registers," which "record[] the numbers dialed on a telephone" (internal quotation marks omitted)).

4. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007) (describing the process of "registration," in which cellular phones "relay their locations to cellular towers").

5. *See id.* (stating that the registration process "occurs roughly every seven seconds when the cell phone is turned on").

6. *Id.*; *see also* 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, 309 (2004) ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

7. *See* McLaughlin, *supra* note 4, at 426 (stating that a single tower location, if located in an urban area, may provide a user's location to within a few hundred feet). An even more precise location can be gained by using triangulation, which employs data from three tower locations. *Id.* at 427. For a more in-depth discussion of the technology of CSLI, see *infra* Part II.

8. *See, e.g.*, Lockwood, *supra* note 6, at 310–11 (providing examples of cases in which police used CSLI to help break their cases, and, in some instances, save lives); *see also* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007) (describing one advantage of CSLI as the fact that so many people carry cell phones, thus providing agents with the ability to track more than objects or certain limited classes of people).

9. *See* Lockwood, *supra* note 6, at 309 (stating that one's "signal can move between different cell towers or faces on a single tower, creating a virtual map of [one's] movements").

10. *See, e.g.*, *In re* Application of the 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. (Orenstein), 396 F. Supp. 2d 294, 296 (E.D.N.Y. 2005) (addressing the government's application for cell site information at the origination and termination of calls as well as during the calls); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (same). As of August 1, 2009, a total of thirty-one *available* district court decisions have addressed law enforcement

context can be classified as historical, prospective, or both.[11] A prospective order is sought when law enforcement officials wish to obtain CSLI "as it happens in real time."[12] This variety of data is commonly referred to as "real-time" CSLI.[13] In the alternative, law enforcement officials may opt to try to compel disclosure of historical CSLI, which service providers maintain in their stored records.[14] Historical CSLI allows the government to learn about a suspect's past and often relatively recent whereabouts.[15]

To date, the vast majority of caselaw in this area has addressed law enforcement applications seeking to compel disclosure of real-time CSLI.[16] This jurisprudential disparity is not surprising in light of the higher investigative utility of real-time CSLI—agents obviously prefer a tool that allows them to remain on top of their suspect's every move to one that leaves them several steps behind that suspect.[17] Despite numerous attempts to obtain real-time CSLI and creative statutory argumentation by government attorneys, law enforcement efforts in this area have been largely unsuccessful[18]—the consensus among courts is that the government cannot obtain real-time CSLI absent probable cause, and generally, the government has not been prepared to satisfy this quantum of proof.[19]

---

applications for CSLI. Because many law enforcement applications for CSLI and corresponding judicial decisions are sealed, the real number is likely significantly higher.

11. *See, e.g.*, McLaughlin, *supra* note 4, at 431–33 (discussing the distinction between prospective and historical applications for CSLI).

12. *Id.*

13. *See, e.g.*, *Smith*, 396 F. Supp. 2d at 748–49 (using the terms "prospective" and "real-time" interchangeably in defining the issue in the case).

14. *See* McLaughlin, *supra* note 4, at 431 (describing historical CSLI applications as law enforcement attempts to "go through the retained records of the service provider").

15. *See id.* (defining the government's goal in historical CSLI applications as "reconstruct[ing] a picture of where a suspect was at a given time in the past").

16. As of August 1, 2009, a total of thirty-one available decisions have addressed law enforcement applications for CSLI. Of these, three involved applications for historical CSLI alone, twenty-five involved applications for real-time CSLI alone, and three involved applications for both. In all subsequent footnotes providing figures on the numbers of certain types of CSLI cases, the figures are current as of August 1, 2009.

17. *See supra* note 12 and accompanying text (describing real-time CSLI as providing law enforcement with location information as it becomes known).

18. *See infra* Part III.C (discussing the widespread rejection of law enforcement applications for real-time CSLI, including courts' rejection of the government's "hybrid theory").

19. Of the twenty-eight total decisions to address the proper standard for real-time CSLI, twenty have held the proper standard to be probable cause. *Compare In re* Application of the 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. (Orenstein), 396 F. Supp. 2d 294, 296 (E.D.N.Y. 2005) (requiring a showing of probable cause to compel disclosure of real-

This Note addresses a question that for the most part has been overlooked in CSLI jurisprudence and literature: What level of suspicion must federal law enforcement officials establish to obtain a court order to compel the disclosure of *historical* cell phone location information? To date, only a handful of courts have confronted this question directly,[20] and, of those that have, almost all have required satisfaction of the lesser quantum of proof contained in the Stored Communications Act (SCA).[21] Several other courts, faced with applications for

---

time CSLI), *and In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (same), *with In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel. (Kaplan), 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) (requiring that the government satisfy the "specific and articulable facts" standard provided in the Stored Communications Act to compel disclosure of real-time CSLI). For a more detailed discussion of real-time CSLI jurisprudence, see *infra* Part III.C.

20. A total of six cases in five districts directly have addressed the proper standard for the disclosure of historical CSLI. *See* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *1–2 (N.D. Ga. Apr. 21, 2008) (addressing the defendants' motion to suppress historical CSLI evidence that had been ordered disclosed by the magistrate judge under the SCA standard); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't (Lenihan), 534 F. Supp. 2d 585, 588 (W.D. Pa. 2008) (addressing a government application for historical CSLI), *aff'd*, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008); *In re* Applications of the U.S. for an Order Authorizing Continued Use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Location Auth. (Alexander II), 530 F. Supp. 2d 367, 368 (D. Mass. 2007) (addressing a government application for both historical and real-time CSLI); *In re* Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info. (Rosenthal), 622 F. Supp. 2d 411, 412–14 (S.D. Tex. 2007) (same); *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. (Alexander I), 509 F. Supp. 2d 64, 66 (D. Mass. 2007) (addressing a government application for historical CSLI), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007); *In re* Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs. (Lee), No. 1:06-MC-6, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006) (addressing separate government applications for historical and real-time CSLI).

21. 18 U.S.C. §§ 2701–2711 (2006). The SCA permits disclosure of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service," *id.* § 2703(c)(1), upon a governmental showing of "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," *id.* § 2703(d). Most courts faced with applications for disclosure of historical CSLI have applied the SCA standard. *See* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *11 (N.D. Ga. Apr. 21, 2008) (denying the defendants' motion to suppress by accepting the magistrate judge's order disclosing historical CSLI based on the SCA standard); *In re* Applications of the U.S. for an Order Authorizing Continued Use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Location Auth. (Alexander II), 530 F. Supp. 2d 367, 368 (D. Mass. 2007) (allowing the disclosure of historical CSLI under the SCA standard); *In re* Application of the U.S. for an Order: (1) Authorizing the Installation and

real-time CSLI, have agreed, stating in dicta that disclosure of historical CSLI is held to the SCA standard.[22] Taken together, these cases represent the proposition that historical CSLI is different from real-time CSLI in a material way—namely, that the act of *storing* location information somehow means that the disclosure of such information is not entitled to the same level of judicial oversight. Until recently, this proposition stood unchallenged.[23]

A recent decision by a United States Magistrate Judge in Pennsylvania, however, has defied this understanding, thereby reanimating what appeared to be a dead issue.[24] In a thorough opinion, Judge Lenihan of the Western District of Pennsylvania held that the disclosure of historical CSLI is governed not by the "specific and articulable facts" standard of the SCA,[25] but by the traditional requirement of probable cause.[26] Unlike the lone other magistrate judge

---

Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info. (Rosenthal), 622 F. Supp. 2d 411, 417 (S.D. Tex. 2007) (same); *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (same).

22. *See In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace 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) (stating that the SCA allows the government to obtain historical CSLI at its lower standard); *Smith*, 396 F. Supp. 2d at 759 n.16 ("[H]istorical cell site data more comfortably fits the category of transactional records covered by [and held to a lower standard by] the SCA."); *Orenstein*, 396 F. Supp. 2d at 307 n.10 ("I have no doubt that the SCA authorizes a service provider's disclosure to law enforcement of historical cell site information . . . .").

23. *But see In re* Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs. (Lee), No. 1:06-MC-6, 2006 WL 1876847, at *5 (N.D. Ind. July 5, 2006) (rejecting the government's request for an order compelling the disclosure of both historical and real-time CSLI, finding that probable cause is required for both). Though this decision held that historical CSLI cannot be disclosed absent probable cause, its holding as to historical CSLI cannot be taken literally because it was based upon an analysis that conflated the two categories (historical and real-time) into one without explanation. *See id.* at *1 ("Either way, the Government [requests] an order requiring cellular phone companies to identify the specific cell tower from which a call originates, is maintained, or received for an incoming or outgoing call. . . . [T]his Court agrees . . . that such information is unobtainable absent a warrant."). More importantly, the court's opinion focused exclusively on real-time CSLI with almost no mention of historical data, suggesting that the holding as to historical CSLI was simply an afterthought.

24. *See Lenihan*, 534 F. Supp. 2d 585, 586 (W.D. Pa. 2008) (holding, in a case involving an application to compel disclosure of historical CSLI, that the government could not obtain such information absent a showing of probable cause).

25. *See* 18 U.S.C. § 2703(d) (2006) (requiring the government to establish "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").

26. *See Lenihan*, 534 F. Supp. 2d at 587 ("[T]his Court holds that the SCA . . . does not authorize access to an individual's cell-phone-derived 'location information,' either past or

decision reaching this conclusion,[27] Judge Lenihan's decision was affirmed by the reviewing district court judge.[28]

Judge Lenihan's decision and the question it revives—whether disclosure of historical CSLI is governed by probable cause or some lesser standard—are significant for several reasons. Law enforcement attempts to obtain real-time CSLI have been, for the most part, unsuccessful.[29] Given the incredibly high investigative utility of CSLI,[30] however, it is unlikely that the failure to obtain real-time CSLI will deter law enforcement officials from pursuing cell phone location data. The more likely outcome is that federal agents more frequently will attempt to obtain *historical* CSLI because old location information certainly is more useful than having no location information at all. As a result, the question of what standard governs the disclosure of historical CSLI likely will become increasingly important in the years to come.[31]

In addition, the novelty of Judge Lenihan's decision suggests that it may influence how future courts address applications requesting historical CSLI. Although several courts have found (either explicitly or in dicta) that historical CSLI is held to a lower standard because it is materially distinguishable from real-time CSLI,[32] Judge Lenihan's decision provides the first substantive defense of the opposing argument. According to this view, the arguments that

---

prospective, on a simple showing of articulable relevance to an ongoing investigation (a 'reasonable relevance' standard).").

27. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. (Alexander I), 509 F. Supp. 2d 64, 66 (D. Mass. 2007) (finding that historical CSLI cannot be disclosed to law enforcement agents in the absence of probable cause). Judge Alexander's decision was reversed on review by the district court. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 81–82 (D. Mass. 2007) (granting the government's application for the disclosure of historical CSLI at the SCA's lesser standard).

28. *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, No. 07-524M, 2008 WL 4191511, at *1 (W.D. Pa. Sept. 10, 2008) (affirming the decision of Magistrate Judge Lenihan that required a showing of probable cause to compel the disclosure of historical CSLI).

29. *See supra* notes 18–19 and accompanying text (noting that the vast majority of courts have required probable cause to compel disclosure of real-time CSLI and that, in practice, this usually has meant the rejection of law enforcement applications for real-time CSLI).

30. *See supra* notes 8–9 and accompanying text (describing the ways in which CSLI can aid in law enforcement investigations, including its usefulness in tracking suspects).

31. In fact, the Department of Justice views the issue as so important that it has appealed Judge Lenihan's ruling and the district court decision affirming it. As of August 1, 2009, that appeal remains pending before the United States Court of Appeals for the Third Circuit.

32. *See supra* notes 21–22 and accompanying text (citing to cases that have said, either explicitly or in dicta, that the SCA's lesser standard governs the disclosure of historical CSLI).

require real-time CSLI to be protected by a probable cause standard apply with equal force to historical CSLI.[33]

This Note defends the view put forth in Judge Lenihan's opinion, arguing that historical CSLI, like real-time CSLI, cannot be disclosed absent a showing of probable cause. Through a detailed analysis of the relevant arguments, including but not limited to those asserted in Judge Lenihan's opinion, it sets forth to debunk the seemingly widely accepted view that stored cell phone location data is entitled to reduced statutory and constitutional protection. In furtherance of this objective, Part II of this Note begins with a brief explanation of the technology that produces CSLI. Part III provides an overview of the legal framework governing the disclosure of CSLI, including federal statutes, Fourth Amendment jurisprudence, and real-time CSLI jurisprudence. Part IV of the Note then addresses the arguments for and against the adoption of a probable cause standard for the disclosure of historical CSLI. More specifically, it compartmentalizes the broader arguments into smaller points of contention, addressing the perspectives of both sides of the debate through this narrower lens. Part V suggests that congressional intervention is needed to resolve this dispute and proposes specific legislation designed to govern judicially-compelled disclosure of CSLI. Finally, on the basis of the arguments presented in Part IV, Part VI of this Note concludes that federal courts cannot compel disclosure of historical CSLI in the absence of probable cause.

II. The Technology of Cell Site Location Information

The legal arguments surrounding CSLI disclosure are premised upon an understanding of the technology that produces such information. Accordingly, a brief technological overview is necessary. The first step in the process that produces CSLI is "registration," the procedure in which a cell phone communicates its location to nearby cellular towers.[34] Registration occurs approximately every seven seconds while a cell phone is turned on and requires no action on the part of the user.[35] Given the automatic nature of the

33. *See Lenihan*, 534 F. Supp. 2d 585, 601 (W.D. Pa. 2008) (rejecting the argument that the relevant statutes and jurisprudence mandate a distinction between real-time and historical CSLI).

34. *See* McLaughlin, *supra* note 4, at 426 (describing the registration process as one in which "[c]ell phones constantly relay their locations to cellular towers").

35. *See id.* ("This process, called 'registration,' occurs roughly every seven seconds when the cell phone is turned on; the user of the phone does not need to take any action . . . .").

registration process, the only way to prevent a phone from conveying location information is to turn the phone off.[36]

As a user moves farther from one cellular tower and closer to another, thereby decreasing signal strength at the first tower while increasing it at the second, her phone will re-register at the nearer tower to ensure the strongest possible signal for sending and receiving calls and messages.[37] In many instances, monitoring these tower switches alone makes it possible to map the movements of particular cell phones, and, consequently, their users.[38] "When two or more towers receive signals from the same phone," however, allowing for a comparative assessment of signal strength, two more precise methods for determining a cell phone's location become available: Time Difference of Arrival (TDOA) and Angle of Arrival (AOA).[39]

TDOA approximates a cell phone's location by measuring the amount of time it takes a signal to travel from the phone to the tower or from the tower to the phone, depending on where the communication is initiated.[40] From such time measurements, it is possible "to estimate the distance between the tower and the phone."[41] When TDOA data is available from multiple towers, CSPs can calculate a phone's latitudinal and longitudinal coordinates.[42] AOA technology, by contrast, determines a phone's location based on the angle at which its signal reaches the tower.[43] "When multiple towers receive signals, [CSPs] can compare the angles of arrival and thus [ascertain] the relative location of the cell phone."[44] When TDOA or AOA data is available from the *three* towers nearest to the cellular device—a possibility referred to as "triangulation"—CSPs are able to provide their most detailed portrayal of a cell phone user's whereabouts.[45]

Monitoring the location of a cellular device—regardless of the method used to approximate that location—allows authorities to pinpoint a user's whereabouts with

---

36. *See id.* ("The only way to stop these signals is to turn the phone off.").

37. *See id.* (describing the process by which towers continually measure signal strength and by which cell phones switch frequencies to obtain a signal from a closer tower); Lockwood, *supra* note 6, at 309 ("If a user has moved to another cell location, the unit re-registers there.").

38. *See, e.g.*, Lockwood, *supra* note 6, at 309 (noting that when a signal moves between different cell towers or between faces of a particular tower, the location information produced can "creat[e] a virtual map of [a user's] movements").

39. *See id.* at 308 (introducing the two processes by which cellular phone towers can approximate cellular phone location).

40. *Id.* at 308–09.

41. *Id.* at 309.

42. *See id.* ("When more than one tower can do so, an algorithm allows the system to determine coordinates corresponding to the phone's latitude and longitude.").

43. *Id.*

44. *Id.*

45. McLaughlin, *supra* note 4, at 427.

incredible detail. "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. This location range can be narrowed by 'tracking which 120 degree face of the tower is receiving a cell phone's signal.'"[46] From there, an *even more specific* location can be determined by triangulating data from the three towers nearest to the device.[47] In rural areas, CSLI provides significantly less detail because there are fewer cellular towers and because the towers that do exist are too spread out to pinpoint a phone's location with much accuracy.[48] In any event, the startling level of precision with which CSLI can be used to identify users' locations—and, over time, to map a history of users' movements—makes clear that such information represents a considerable invasion upon individual privacy.

III. The Law Governing the Disclosure of CSLI

This Part discusses the relevant background law that governs law enforcement applications for the disclosure of CSLI. Part III.A begins with a description of the applicable federal statutory framework. Part III.B discusses pertinent Fourth Amendment jurisprudence, including the Supreme Court's assumption of the risk and tracking beeper cases. Part III.C concludes with a summary of the case law on applications for real-time CSLI, noting that district courts have widely held that such data cannot be disclosed absent a governmental showing of probable cause.

A. Statutory Framework

1. The Pen Register Statute

Title III of the Electronic Communications Privacy Act of 1986 (ECPA), commonly referred to as the Pen Register Statute (PRS),[49] applies to law

46. *Lenihan*, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (quoting McLaughlin, *supra* note 4, at 427).

47. *See* McLaughlin, *supra* note 4, at 427 ("A more accurate picture of a phone's location [than that provided by simply knowing the nearest cellular tower] may be generated by using triangulation . . . .").

48. *See id.* at 426 ("In rural areas, towers may be miles apart."); Lockwood, *supra* note 6, at 309 ("In rural settings, the location information available to providers is significantly less accurate simply because fewer towers are available. In some areas, cell service is provided by a single tower covering several hundred square miles.").

49. Electronic Communications Privacy Act of 1986 § 301, 18 U.S.C. §§ 3121–3127 (2006).

enforcement applications for two forms of telephone-based surveillance: pen registers and trap and trace devices.[50] Judge Lenihan aptly summarized each of these surveillance devices, including their critical difference:

> [A] "Pen Register" is a device which records or decodes electronic or other impulses which identify the telephone numbers dialed or otherwise transmitted on the telephone line to which such device is attached (*i.e.*, the numbers of *outgoing* calls). A trap and trace device captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted (*i.e.*, the numbers of *incoming* calls).[51]

Under the PRS, the government must obtain a court order before installing a pen register or a trap and trace device on a suspect's phone.[52] Despite this prohibition, the PRS sets a low bar for obtaining such an order: The court merely must find, upon certification by a government attorney, "that the information likely to be obtained by [installing and using the device] is relevant to an ongoing criminal investigation."[53] Court orders allowing the use of pen registers and trap and trace devices are limited in duration—they cannot exceed sixty days—but may be extended in the event of an additional application by the government.[54]

2. The Stored Communications Act

The Stored Communications Act, which constitutes Title II of the Electronic Communications Privacy Act of 1986,[55] regulates the disclosure of stored wire and electronic communications information.[56] The SCA divides

---

50. *See, e.g.*, *id.* § 3121(a) (providing general prohibition on the installation and use of pen registers or trap and trace devices without a court order).

51. *Lenihan*, 534 F. Supp. 2d at 593. *Accord In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 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.").

52. *See* § 3121(a) ("Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order . . . .").

53. *Id.* § 3123(a)(1).

54. *See id.* § 3123(c) (defining the temporal limit for court orders that allow for the installation of pen registers or trap and trace devices and providing a provision for extending orders beyond that limit).

55. Electronic Communications Privacy Act of 1986 § 201, 18 U.S.C. §§ 2701–2711 (2006).

56. *See, e.g.*, *id.* § 2701(a) (providing general criminal prohibition on unauthorized access

communications information sought by the government into two mutually exclusive categories: the contents of communications[57] and "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service (not including the contents of communications)."[58] More importantly, it dictates the steps the government must take to compel the disclosure of each of these varieties of information.[59] Because CSLI does not constitute the contents of communications, the portion of the SCA relevant to its disclosure is that which addresses disclosure of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service."

Section 2703(c) provides the guidelines for compelled disclosure of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service."[60] Aside from governmental requests for the disclosure of certain specified pieces of information[61] and for information "relevant to a law enforcement investigation concerning telemarketing fraud,"[62] § 2703(c) provides the government with three routes to compelled disclosure.[63] First, law enforcement agents can obtain a warrant under the Federal Rules of Criminal Procedure.[64] Alternatively, the government may obtain "the consent of the subscriber or customer to such

---

to stored wire or electronic communications); *id.* § 2703 (referring only to wire and electronic communications in delineating the Act's disclosure rules).

57. *See id.* §§ 2703(a)–(b) (providing the requirements the government must satisfy to compel disclosure of *contents* of electronic communications information held in electronic storage and remote computing services, respectively).

58. *Id.* § 2703(c).

59. *See id.* §§ 2703(a)–(c) (delineating the requirements for compelled disclosure of electronic communications information in three specific instances); *id.* § 2703(d) (providing a different requirement for the disclosure of information falling under specified portions of subsections (b) and (c)).

60. *Id.* § 2703(c).

61. *See id.* § 2703(c)(2) (requiring service providers to disclose to the government the name, address, telephone records, length of service, telephone number, and source of payment if demanded by the appropriate form of subpoena).

62. *Id.* § 2703(c)(1)(D).

63. *See infra* notes 64–67 and accompanying text (describing the three means of disclosure under § 2703(c): obtaining a warrant, satisfying § 2703(d), and procuring the consent of the subscriber or customer).

64. *See* 18 U.S.C. § 2703(c)(1)(A) (2006) (permitting disclosure of a "record or other information pertaining to a subscriber" if the government obtains a warrant). Under the Federal Rules of Criminal Procedure, the general rule is that warrants will not be issued absent probable cause. *See* FED. R. CRIM. P. 41(d)(1) ("[A] magistrate judge . . . must issue [a] warrant if there is probable cause to search for . . . a person or property or to install and use a tracking device.").

disclosure."[65] Finally, it may compel disclosure of "record[s] or other information pertaining to a subscriber" if it receives a court order under § 2703(d).[66] Section 2703(d), in turn, 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.*[67]

The § 2703(d) standard is demonstrably less stringent than the warrant requirement imposed by the Federal Rules of Criminal Procedure, and, by extension, § 2703(c)(1)(A).[68] That, coupled with the fact that no reasonable law enforcement official would sacrifice the element of surprise in her surveillance by seeking a suspect's consent for disclosure, leads to an intuitive three-step approach for law enforcement agents seeking CSLI: (1) argue that the SCA applies to CSLI; (2) argue that CSLI qualifies under § 2703(c) as "a record or other information pertaining to a subscriber;" and (3) assert that CSLI therefore can be disclosed under the less stringent § 2703(d) standard. In fact, this is a major part of the argument relied upon by the government.[69]

As previously mentioned, the SCA only applies to the disclosure of wire or electronic communications.[70] Because cellular communications, and thus CSLI, clearly are not a form of wire communication,[71] the SCA can govern the disclosure of CSLI only if cellular communications can be classified as a form of "electronic communication." Although cellular communications appear to fall within the positive definition of "electronic communication,"[72] the

---

65. 18 U.S.C. § 2703(c)(1)(C).

66. *Id.* § 2703(c)(1)(B).

67. *Id.* § 2703(d) (emphasis added).

68. *Compare id.* (requiring "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a . . . communication . . . or other information sought[] are relevant and material to an ongoing criminal investigation"), *with* FED. R. CRIM. P. 41(d)(1) (requiring probable cause).

69. *See infra* Part III.C (discussing in greater detail the legal arguments made by the government in cases in which it sought to compel the disclosure of real-time CSLI).

70. *See supra* note 56 (providing examples of provisions in the SCA that illustrate that the Act's scope is limited to wire and electronic communications).

71. *See* 18 U.S.C. § 2510(1) (2006) (defining the term "wire communication" as "any aural transfer made in whole or in part . . . by the aid of *wire, cable, or other like connection* between the point of origin and the point of reception" (emphasis added)).

72. *See id.* § 2510(12) (defining the term "electronic communication" to include "any transfer of . . . sounds[] [or] data . . . transmitted in whole or in part by a . . . radio, electromagnetic, photoelectronic or photooptical system").

definition also contains a negative component that excludes from its reach "any communication from a tracking device."[73] The term "tracking device" is defined as "an electronic or mechanical device which *permits* the tracking of the movement of a person or object."[74] In other words, the government may not rely on the SCA to compel disclosure of non-wire forms of communication that derive from devices that *can be used* to determine the movements of their users. For obvious reasons, opponents of CSLI-based surveillance have placed significant emphasis on this exception.[75]

3. *The Communications Assistance for Law Enforcement Act*

In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA),[76] legislation that requires "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,"[77] among other things:

> [E]xpeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access *call-identifying information* that is reasonably available to the carrier (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and (B) in a manner that allows it to be associated with the communication to which it pertains.[78]

More importantly for purposes of CSLI disclosure, this requirement is subject to an exception; telecommunications carriers must be capable of providing the information described above, but with one limitation:

> [W]ith regard to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18), such call-identifying information *shall not include any information*

---

73. *Id.* § 2510(12)(C).

74. *Id.* § 3117(b) (emphasis added).

75. *See infra* Part IV.A.1.a (setting forth the arguments for and against applying the tracking device exception to historical CSLI).

76. Communications Assistance for Law Enforcement Act §§ 102–112, 47 U.S.C. §§ 1001–1010 (2000).

77. 47 U.S.C. § 1002(a).

78. *Id.* § 1002(a)(2) (emphasis added).

> *that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number).[79]

The CALEA defines the term "call-identifying information" 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."[80] Because the terms "wire communication" and "electronic communication" are defined in the same way under the CALEA as they are under the SCA,[81] communications from devices that can be used to track an individual's movements are not "electronic communications" under the CALEA.[82]

The legislative history surrounding the CALEA's exception for information that reveals a user's location is among the many contentious issues in CSLI scholarship and jurisprudence.[83] In enacting the CALEA, Congress's objective was to balance its interest in aiding effective law enforcement with its interest in "protect[ing] privacy in the face of increasingly powerful and personally revealing technologies."[84] This privacy interest ultimately proved to be paramount to Congress, as legislators expressed grave concerns that the enactment of the CALEA would change the "background requirements" governing disclosure of sensitive telecommunications information and would "later [be] asserted to have affected the judicial review protections applicable to" such information.[85] These fears were allayed by the testimony of then-FBI Director Louis Freeh, who appeared before both the Senate and the House of Representatives to testify regarding how law enforcement officials understood and intended to apply the Act.[86] First, Director Freeh told Congress that the

---

79. *Id.* (emphasis added).

80. *Id.* § 1001(2).

81. *See id.* § 1001(1) ("The terms defined in [18 U.S.C. § 2510] have, respectively, the meanings stated in that section."). "Wire communication" and "electronic communication" are each defined in 18 U.S.C. § 2510. 18 U.S.C. §§ 2510(1), 2510(12) (2006). Like the CALEA, the SCA relies upon the § 2510 definitions. *See id.* § 2711(1) ("[T]he terms defined in [18 U.S.C. § 2510] have, respectively, the definitions given such terms in that section.").

82. *See supra* notes 73–74 and accompanying text (explaining the tracking device exception).

83. *See infra* Part IV.A.3 (discussing the debate regarding how the CALEA, and particularly its legislative history, should be understood).

84. H.R. REP. NO. 103-827, at 13 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3493. In addition to its interest in protecting privacy, Congress defined its other two interests as "preserv[ing] a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts," and "avoid[ing] impeding the development of new communications services and technologies." *Id.*

85. *Lenihan*, 534 F. Supp. 2d 585, 596 (W.D. Pa. 2008).

86. *See id.* (describing Director Freeh's participation as involving "lengthy and repeated

CALEA was not intended to make it possible for law enforcement agents to obtain location information or to otherwise expand the government's then-existing authority to obtain private telecommunications information.[87] Freeh also declared that law enforcement officials had "no intent whatsoever . . . to acquire anything [under the CALEA] that could properly be called 'tracking' information."[88] Most importantly, Director Freeh recommended that Congress add an exception to what is now § 1002(a)(2) for information revealing a subscriber's location, noting that such an exception would alleviate any concerns that pen registers, trap and traces, and similar devices could be used to acquire location or movement information.[89] As indicated above, Congress followed this suggestion and excluded from the CALEA's requirements the disclosure of any location-identifying information.[90]

B. Relevant Fourth Amendment Jurisprudence

1. The Fourth Amendment Definition of "Search"

The Fourth Amendment to the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[91] As the text of the Amendment indicates, the Fourth Amendment applies only when a governmental action can be classified as either a "search" or a "seizure."[92] Justice Harlan provided the classic definition of "search" in his concurrence in

---

testimony before [both] the Senate and House").

87. *See id.* (asserting that Freeh "reassured Congress" that "the proposed legislation would 'ensure[] the maintenance of the status quo'" (quoting *Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecomms. Techs. and Servs.: Hearings Before the Subcomm. on Tech. and Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 2, 28 (1994) [hereinafter *CALEA Joint Hearings*] (statement of Louis Freeh, Director, Federal Bureau of Investigation))).

88. *Id.* (quoting *CALEA Joint Hearings*, *supra* note 87, at 23 (statement of Louis Freeh, Director, Federal Bureau of Investigation)).

89. *See id.* at 597 (noting that Director Freeh represented that law enforcement officials were comfortable with adding the exception now codified at 47 U.S.C. § 1002(a)(2) (citing *CALEA Joint Hearings*, *supra* note 87, at 29 (statement of Louis Freeh, Director, Federal Bureau of Investigation))).

90. *See supra* note 79 and accompanying text (discussing the CALEA's limitation on the disclosure of location-identifying information obtained solely pursuant to the PRS).

91. U.S. CONST. amend. IV.

92. *See id.* (defining the right as the protection from "unreasonable searches and seizures").

the judgment in *Katz v. United States*:[93] "[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.'"[94] If either prong of the test fails—if the asserted expectation of privacy either could not have been subjectively held by the individual alleging a search or is an expectation that society would not view as reasonable—then no search has taken place and the Fourth Amendment is not implicated.[95]

2. Assumption of the Risk

In *United States v. Miller*,[96] the Supreme Court addressed whether a bank's disclosure of a customer's records, when compelled by the government, constitutes a search under the Fourth Amendment.[97] In *Miller*, the government used subpoenas to compel two banks to disclose all records of accounts in the defendant's name during a particular time period.[98] Although the defendant argued that he had a reasonable expectation of privacy in the personal records he provided to the banks,[99] the Court disagreed.[100] The Court first noted that the documents disclosed by the bank could not be deemed the defendant's "private papers."[101] It then explained why it found no legitimate expectation of privacy in the information in question, which the bank had obtained only because the defendant had supplied it: "All of the documents obtained,

---

93. *See* Katz v. United States, 389 U.S. 347, 353, 359 (1967) (concluding that the government's placing of a wiretap on a public phone booth to record the contents of the defendant's phone call constituted a search, and finding that the government's failure to obtain judicial authorization prior to engaging in that search violated the Fourth Amendment).

94. *Id.* at 361 (Harlan, J., concurring).

95. *See id.* (defining the term "search" to encompass two requirements, each of which must be met to trigger the protection of the Fourth Amendment).

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

97. *See id.* at 439–40 (noting and accepting the government's argument that the defendant had no Fourth Amendment privacy interest in his bank records).

98. *See id.* at 437–38 (discussing the bank records obtained by the government in the case).

99. *See id.* at 442 ("Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy.").

100. *Id.* ("[W]e perceive no legitimate 'expectation of privacy' in their contents.").

101. *Id.* at 440 ("On their face, the documents subpoenaed here are not respondent's 'private papers.'").

including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[102] The Court then took the added step of couching its holding in terms of assumption of the risk:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [that third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[103]

Because the Court found that the defendant lacked a legitimate expectation of privacy in the information he provided to the banks, it concluded that no search had taken place and that, therefore, the defendant "possessed no Fourth Amendment interest."[104]

The Court reached a similar outcome in *Smith v. Maryland*,[105] a case that addressed "the question whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment."[106] As noted above, a pen register is a device that records the numbers dialed from a particular phone.[107] The Court in *Smith* described pen registers as minimally intrusive in that they acquire only the numbers dialed from particular phones—not the contents of the communications emanating from those phones.[108] In light of this limitation, the Court characterized the defendant's Fourth Amendment argument as a simple "claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[109]

The *Smith* Court rejected this claim. First, it found that people are unlikely to have any subjective expectation of privacy in the numbers they dial:

---

102. *Id.* at 442.

103. *Id.* at 443 (citations omitted).

104. *Id.* at 445.

105. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (concluding that "[t]he installation and use of a pen register . . . was not a 'search'" because the defendant lacked any reasonable expectation of privacy in the phone numbers he dialed).

106. *Id.* at 736.

107. *See supra* note 51 and accompanying text (defining the term "pen register").

108. *See Smith*, 442 U.S. at 741 ("These devices do not hear sound. They disclose only the telephone numbers that have been dialed . . . . Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977))).

109. *Id.* at 742.

"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 . . . ."[110] Second, the Court declared that even if the defendant had an actual expectation of privacy, his expectation could not be deemed reasonable because of the assumption of the risk doctrine.[111] Referring to the analogous situation in *Miller*, the Court stated:

> This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[112]

Based on this rationale, the *Smith* Court concluded that the installation and use of a pen register does not constitute a "search" for purposes of the Fourth Amendment.[113]

3. The Tracking Beeper Cases

The Supreme Court addressed the Fourth Amendment legality of law enforcement use of tracking beepers in a pair of cases decided only one year apart: *United States v. Knotts*[114] and *United States v. Karo*.[115] As the Court explained in *Knotts*, "[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."[116] By using such devices, law enforcement agents—the recipients of the beepers'

---

110. *Id.* at 743.

111. *See id.* at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

112. *Id.* at 744.

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

114. *See* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding that no search occurred because the government's use of a tracking beeper disclosed no information that officers could not have otherwise obtained simply by following the suspect's public movements).

115. *See* United States v. Karo, 468 U.S. 705, 715 (1984) (finding that the government's use of a tracking beeper constituted a search to the extent that it revealed information about the interior of a private residence).

116. *Knotts*, 460 U.S. at 277.

signals—are able to track the locations of the objects on or in which they are placed.[117]

The police in *Knotts*, having learned that a suspected manufacturer of methamphetamine was purchasing chemicals from a particular company, obtained the consent of that company to place a tracking beeper within a container of chloroform prior to its purchase by the suspect.[118] After observing the suspect make the purchase, officers followed the suspect's car by way of visual surveillance and use of the tracking beeper.[119] Eventually, the officers lost both visual surveillance and the signal from the beeper.[120] When they recovered the signal about one hour later, they found that it had come to rest near a secluded cabin owned by Knotts.[121] Importantly, "after the location *in the area of the cabin* had been initially determined," law enforcement agents ceased their use of the beeper.[122] Based largely upon tracking the chloroform to the cabin, officers were able to secure a search warrant for the premises.[123]

The *Knotts* Court ruled that no search had taken place because the way in which the police had used the tracking beeper had not invaded any reasonable expectation of privacy.[124] It began its analysis by pointing out that the defendant was attempting to assert a privacy interest in conduct that was of a public nature: "The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways."[125] In light of this characterization, the Court made clear that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to

117. *See, e.g., id.* at 278 (describing how officers used the tracking beeper to follow the container of chloroform in which they had placed the beeper).

118. *See id.* (describing the circumstances that gave rise to the installation of the tracking beeper by law enforcement).

119. *See id.* ("When Armstrong made the purchase, officers followed the car in which the chloroform had been placed, maintaining contact by using both visual surveillance and a monitor which received the signals sent from the beeper.").

120. *See id.* (stating that "the pursuing agents ended their visual surveillance" and "[a]t about the same time . . . lost the signal from the beeper").

121. *See id.* (describing how officers rediscovered the signal and identified the defendant's cabin as its stationary location).

122. *Id.* at 278–79 (emphasis added).

123. *See id.* at 279 ("Relying on the location of the chloroform derived through the use of the beeper and additional information obtained during . . . intermittent visual surveillance of respondent's cabin, officers secured a search warrant.").

124. *See id.* at 285 (holding that police monitoring of tracking beeper signals under the facts of the case did not "invade any legitimate expectation of privacy" held by the defendant).

125. *Id.* at 281.

another."[126] Although the Court conceded that the defendant had a legitimate expectation of privacy in the cabin itself, it declared that this expectation did not encompass "the visual observation of [his accomplice's] automobile arriving on his premises after leaving a public highway."[127] As these passages indicate, the Court focused heavily on the fact that police could have learned everything that the beeper disclosed to them—namely, that the container ended up at the defendant's cabin—simply by observing the driver's movements in public.[128] Relying on this same rationale, the Court concluded by rejecting the defendant's argument that the failure of the government's visual surveillance meant that their use of the beeper to find the cabin invaded a protected sphere of privacy:

> Admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes. But scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise. A police car following [the driver] at a distance throughout his journey *could have observed* him leaving the public highway and arriving at the cabin owned by respondent with the drum of chloroform still in the car. . . . [T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.[129]

Because the defendant was attempting to claim a Fourth Amendment interest in information that officers *could have* observed publicly, the Court concluded that the defendant's asserted expectation of privacy was not reasonable and that, accordingly, no search had taken place.[130]

One year later in *United States v. Karo*, the Court imposed an important limitation on the holding in *Knotts*.[131] In *Karo*, police obtained a court order—later declared invalid—to install a beeper on a container of ether after learning from an informant that the defendant and others were prepared to purchase a significant amount of that chemical for the purpose of extracting cocaine from

---

126. *Id.*

127. *Id.* at 282.

128. *See id.* ("Visual surveillance from public places along [the driver's] route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police.").

129. *Id.* at 285 (emphasis added).

130. *See supra* note 124 (describing the Court's ultimate conclusion in *Knotts*).

131. *See* United States v. Karo, 468 U.S. 705, 715 (1984) (finding that the government's use of a tracking beeper was a "search" because it revealed information about the interior of a home).

clothing.[132] Officers observed the defendant make the purchase and followed him to his home using both visual surveillance and the beeper.[133] Later that day, agents relied upon the beeper to ensure that the container was still in the defendant's home.[134] In the ensuing weeks and months, police continued to utilize the beeper to track the frequent movements of the ether among the defendant's accomplices, using it two other times to determine its presence in private locations.[135] In the first instance, officers relied upon the beeper to approximate that the chemicals were being held in a commercial storage unit rented by one of the defendant's accomplices.[136] Later, after observing that the chemicals had been transported to a home occupied by three of the defendant's accomplices, agents twice used the beeper to ensure that the ether remained in that residence.[137] On the basis of this information, law enforcement officials secured a warrant to search the residence in which the chemicals came to rest.[138]

The Court swiftly distinguished *Karo*'s facts from those in *Knotts*. It noted that unlike the law enforcement agents in *Knotts*, the agents in *Karo* had used a tracking beeper to locate the item *within a particular residence*, a fact that agents readily conceded in their search warrant application.[139] In light of this distinction, the *Karo* Court asked "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."[140] The Court concluded that this more intrusive form of monitoring constitutes a search that, when conducted without a warrant, violates the Fourth Amendment.[141]

---

132. *See id.* at 708 (describing the circumstances under which the police initiated their beeper-based surveillance).

133. *See id.* ("[A]gents saw Karo pick up the ether . . . . They then followed Karo to his house using visual and beeper surveillance.").

134. *See id.* ("At one point later that day, agents determined by using the beeper that the ether was still inside the house . . . .").

135. *See id.* at 708–09 (recounting the continued movements of the ether and the agents' use of the tracking beeper to keep up with those movements).

136. *See id.* at 708 ("Using the beeper, agents confirmed that the ether was indeed in one of the lockers in the row containing [the locker rented by an accomplice of the defendant] . . . .").

137. *See id.* at 709–10 ("[A]gents determined, using the beeper monitor, that the beeper can was still inside the house. Again [the next day], the beeper revealed that the ether can was still on the premises.").

138. *Id.* at 710.

139. *See id.* at 714 ("[T]he beeper was used to locate the ether in a specific house in Taos, NM, and . . . that information was in turn used to secure a warrant for the search of the house.").

140. *Id.*

141. *See id.* (finding that "the monitoring of a beeper in a private residence . . . not open to

Citing the heightened level of privacy guaranteed to the home under the Fourth Amendment, the *Karo* Court stated that the use of the beeper in this case told agents "that a particular article [was] actually located at a particular time in the private residence and [was] in the possession of the person or persons whose residence [was] being watched."[142] This, said the Court, is as offensive to the Fourth Amendment as an agent entering the residence without a warrant to see if the item is actually inside.[143] Again emphasizing the difference between its facts and those in *Knotts*, the Court characterized the surveillance here as "reveal[ing] a critical fact about the interior of the premises that the Government [was] extremely interested in knowing and that it could not have otherwise obtained without a warrant."[144] After providing this rationale, the Court concluded by rejecting a government argument that is particularly relevant in the CSLI context:

> If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the Government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they will have no way of knowing in advance whether the beeper will be transmitting its signals from inside private residences. The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.[145]

Taken together, *Knotts* and *Karo* establish a "public/private dichotomy" that governs the Fourth Amendment validity of law enforcement use of tracking devices.[146] The result of these cases is that "a warrant is constitutionally required if and only if the location information extends onto private property."[147] Thus, in the absence of a warrant, "the Government may use a tracking device to ascertain an individual's location on a public highway but not in a private home."[148]

---

visual surveillance[] violates the Fourth Amendment rights" of individuals with privacy interests in the residence).

142. *Id.* at 715.

143. *See id.* (comparing the surveillance in question to warrantless physical intrusions into the home and finding that "[f]or purposes of the Amendment, the result is the same" because the government acted without a warrant "to obtain information that it could not have obtained by observation from outside the . . . house").

144. *Id.*

145. *Id.* at 718.

146. *See Lenihan*, 534 F. Supp. 2d 585, 613 (W.D. Pa. 2008) ("[T]he public/private dichotomy is the principle harmonizing *Knotts* and *Karo* . . . .").

147. *Id.*

148. *Id.*

C. Real-time CSLI Jurisprudence: Widespread Rejection of the Hybrid Theory

As previously indicated, there has been a significant amount of litigation at the district court level regarding what standard governs the disclosure of real-time CSLI.[149] In most of this litigation, the Government has sought to compel disclosure of real-time CSLI by combining various pieces of electronic surveillance law, including selected provisions of the PRS, the SCA, and the CALEA.[150] This approach is known as the "hybrid" or "dual authority" theory.[151]

The government's hybrid theory argument rests upon three premises.[152] First, the government asserts that the USA PATRIOT Act[153] expanded the PRS definitions of "pen register" and "trap and trace device" in such a way that CSLI is now obtainable under the PRS.[154] Specifically, the government notes that these terms now encompass "signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,"[155] a category that it feels includes CSLI.[156] The second step in the government's argument arises from the CALEA's prohibition on obtaining location information "solely pursuant to" the PRS.[157] Focusing on the "solely

149. *See supra* notes 16–19 and accompanying text (providing a brief synopsis of the state of prospective CSLI jurisprudence).

150. *See, e.g.*, *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 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).

151. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info. (Adelman), No. 06-MISC-004, 2006 WL 2871743, at *3 (E.D. Wis. Oct. 6, 2006) ("Courts have characterized this as a 'hybrid' or 'dual authority' theory . . . .").

152. *See, e.g.*, *In re* Application of the 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. (McGiverin), 497 F. Supp. 2d 301, 306–09 (D.P.R. 2007) (working through the three steps that make up the government's "hybrid theory" argument).

153. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

154. *See McGiverin*, 497 F. Supp. 2d at 306 (noting the government's assertion that CSLI falls within the PRS because that statute now defines "pen register" as a device that can record "signaling information").

155. 18 U.S.C. § 3127(3) (2006).

156. *See, e.g.*, *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel. (Kaplan), 460 F. Supp. 2d 448, 455 (S.D.N.Y. 2006) (accepting the government's argument that CSLI "is 'signaling information' within the meaning of the Pen Register Statute").

157. *See, e.g.*, *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen

pursuant to" language, the government claims that the CALEA permits law enforcement to obtain location information using the PRS in conjunction with another statute.[158] The final premise in the hybrid theory argument is that "the Stored Communications Act provides the additional authority required by CALEA."[159] From these premises, the government concludes that it may compel disclosure of real-time CSLI when it satisfies the SCA's disclosure standard,[160] which it does when it provides "specific and articulable facts showing that there are reasonable grounds to believe that the . . . [CSLI] sought [is] relevant and material to an ongoing criminal investigation."[161]

Generally, the government has had very little success in compelling the disclosure of real-time CSLI by way of its hybrid theory argument.[162] Courts that reject the theory primarily do so by casting doubt on one or more of its premises. Although most courts do not question the government's first premise—that CSLI falls within the post-PATRIOT Act scope of the PRS—at least one judge argues against it.[163] Judge Smith contends that the PATRIOT Act's expanded pen/trap definitions were intended only to cover communications such as email: "The added term 'dialing, routing, addressing, and signaling information,' while not defined in the statute, was touted by the bill's proponents as a way to update the [PRS] to cover Internet traffic."[164] Judge Smith also questions whether, apart from this legislative history, the new definitions fairly can be read to encompass CSLI, pointing out that information sought under the PRS still must be incident to a "wire or electronic

---

Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info. (Orenstein), 396 F. Supp. 2d 294, 315 (E.D.N.Y. 2005) ("The government recognizes that CALEA bars it from seeking to compel a provider to disclose information via a pen register that reveals a mobile telephone user's location 'solely pursuant to' the [PRS].").

158. *See, e.g.*, *In re* Application of the 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. (McGiverin), 497 F. Supp. 2d 301, 307 (D.P.R. 2007) ("[T]he government . . . contend[s] that the phrase 'solely pursuant' necessarily directs that the [PRS] may be used in combination with some other . . . authority for release of information that may disclose physical location.").

159. *Kaplan*, 460 F. Supp. 2d at 454.

160. *See, e.g.*, *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005) (noting the government's view that CSLI can be obtained under the § 2703(d) "specific and articulable facts" standard).

161. 18 U.S.C. § 2703(d) (2006).

162. *See supra* note 19 and accompanying text (noting that, as of August 1, 2009, twenty of twenty-eight decisions addressing applications for disclosure of real-time CSLI have held the proper standard to be probable cause rather than the standard provided in § 2703(d)).

163. *See Smith*, 396 F. Supp. 2d at 761–62 (arguing that the post-PATRIOT Act definitions in the PRS do not cover CSLI).

164. *Id.* at 761.

communication."[165] Because CSLI is transmitted without the making or receiving of a call, Judge Smith argues that CSLI does not arise out of a wire or electronic communication and thus does not fall within the PRS.[166]

The hybrid theory's second premise—that the CALEA's prohibition on obtaining location information "solely pursuant to" the PRS means that such information can be obtained by using the PRS in conjunction with another statute—also faces criticism.[167] To begin with, opponents of the hybrid theory note that using the PRS in conjunction with another law is not the only way law enforcement agents can obtain prospective CSLI; they also have the option of obtaining a Rule 41 warrant based on probable cause or a wiretap "superwarrant" under 18 U.S.C. § 2518.[168] More fundamentally, opponents of the theory question whether the PRS has any connection to the SCA under federal surveillance law.[169] These courts point out that the CALEA was not intended to expand or alter the existing surveillance options available to law enforcement, but was instead simply meant to ensure that communications providers would be capable of providing surveillance information to law enforcement officials.[170] Opponents further note that FBI Director Freeh testified before Congress that the law has "nothing to do with 'transactional information'" protected by the SCA and that the CALEA "does not relate to [the SCA]."[171] Judge Smith summarized this final basis for rejecting the hybrid theory's second premise: "Far from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the

---

165. *See id.* at 762 ("[T]he expanded definition . . . indicates that . . . 'signaling' information is generated by, and incidental to, the transmission of 'a wire or electronic communication.'").

166. *See id.* (noting that CSLI is recorded without the transmission of any communication).

167. *See infra* notes 168–72 and accompanying text (discussing courts' rejection of the hybrid theory's second premise).

168. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info. (Adelman), No. 06-MISC-004, 2006 WL 2871743, at *4 (E.D. Wis. Oct. 6, 2006) ("[T]here is no reason why the government could not obtain [CSLI] under Rule 41 or 18 U.S.C. § 2518.").

169. *See In re* Application of the 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. (Orenstein), 396 F. Supp. 2d 294, 319–20 (E.D.N.Y. 2005) (noting that the legislative history of the CALEA indicated a clear distinction between the scopes of the PRS and the SCA); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 762–64 (S.D. Tex. 2005) (same).

170. *See Smith*, 396 F. Supp. 2d at 762 ("One of CALEA's main objectives was to allow law enforcement to retain existing surveillance capabilities in the face of technological change . . . .").

171. *Id.* at 763 (quoting *CALEA Joint Hearings*, *supra* note 87, at 27–28 (statement of Louis Freeh, Director, Federal Bureau of Investigation)).

[PRS] 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."[172]

Opponents also take issue with the hybrid theory's third premise, which states that the SCA provides the supplementary authority (in addition to the PRS) that the CALEA requires to obtain location information. On a basic level, courts express qualms about allowing an act governing *stored* communications to be used—even indirectly—to authorize real-time and ongoing surveillance.[173] Furthermore, opponents point out that the core of the SCA is a prohibition on the disclosure of subscriber information to governmental authorities.[174] This general prohibition, they say, is subject to only narrow and specified exceptions, none of which reference the PRS.[175] Given this fundamental proscription on disclosure, opponents declare that the SCA "preclude[s] the very authority law enforcement seeks."[176]

Courts find further reason to reject the hybrid theory's final premise by arguing that the SCA—specifically its § 2703(d) disclosure standard—cannot possibly apply to CSLI.[177] The § 2703(d) standard can apply to CSLI only if the government establishes that CSLI constitutes "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication] service."[178] Accordingly, courts that oppose the hybrid theory argue that CSLI falls outside of this category, specifically because it does not "pertain to" an "electronic communication service."[179] An "electronic

---

172. *Id.* at 764 (quoting *CALEA Joint Hearings*, *supra* note 87, at 27–28 (statement of Louis Freeh, Director, Federal Bureau of Investigation)).

173. *See In re* Application of the 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. (McGiverin), 497 F. Supp. 2d 301, 309 (D.P.R. 2007) ("[T]he SCA, as its title announces, contemplates orders for *stored* rather than prospective information . . . ."); *Orenstein*, 396 F. Supp. 2d at 308 (describing SCA orders as "inherently retrospective"); *Smith*, 396 F. Supp. 2d at 760 ("Unlike other titles of the ECPA, which regulate methods of real-time surveillance, the SCA regulates access to records and communications in storage.").

174. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info. (Adelman), No. 06-MISC-004, 2006 WL 2871743, at *6 (E.D. Wis. Oct. 6, 2006) (noting the SCA's general prohibition and the fact that it is subject to certain exceptions).

175. *See id.* (pointing out the absence of an SCA exception for authorization under the PRS).

176. *Id.*

177. *See infra* notes 178–86 and accompanying text (discussing courts' rejection of the third premise of the hybrid theory).

178. *See supra* notes 60–68 and accompanying text (explaining the SCA's disclosure framework with respect to "records or other information pertaining to a subscriber").

179. *See, e.g.*, *In re* Application of the 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

communication service" exists only when "wire or electronic communications" are transmitted.[180] With respect to CSLI, opponents argue that neither wire nor electronic communications are involved.[181] CSLI (and, more generally, cellular communications) cannot be "electronic communication[s]," they say, because that term excludes communications from "tracking devices."[182] Courts that reject the hybrid theory find that cell phones fall within the definition of "tracking device"[183] because the definition merely requires that the device "*permits the tracking* of the movement of a person or object."[184] Opponents further assert that CSLI cannot be a "wire communication" because it does not require or involve a transfer of the human voice.[185] Because they find that CSLI arises without the transmission of a wire or electronic communication, courts that reject the hybrid theory conclude that CSLI does not "pertain to a subscriber to . . . an [electronic communication] service" and thus cannot be disclosed under the SCA's § 2703(d) standard.[186]

Finally, opponents reject the hybrid theory because they view it as an altogether unwarranted reading of the statutes. This position was best articulated by Judge Smith:

Cell Site Info. (Orenstein), 396 F. Supp. 2d 294, 308 (E.D.N.Y. 2005) (summarizing the reasons why CSLI does not "pertain to" subscribers' use of electronic communication services).

180. *See, e.g., id.* ("'Electronic communication service' must involve the transmission of 'wire or electronic communications.'" (quoting 18 U.S.C. § 2510(15) (2006))).

181. *See, e.g., id.* (stating why CSLI implicates neither wire nor electronic communications).

182. *See, e.g., id.* ("'[E]lectronic communication' excludes 'any communication from a tracking device.'" (quoting 18 U.S.C. § 2510(12)(C) (2006))).

183. *See, e.g., In re* Application of the 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. (McGiverin), 497 F. Supp. 2d 301, 310 (D.P.R. 2007) (finding that cell phones constitute "tracking devices"); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005) (same).

184. 18 U.S.C. § 3117(b) (2006) (emphasis added).

185. *See, e.g., In re* Application of the 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. (Orenstein), 396 F. Supp. 2d 294, 308 (E.D.N.Y. 2005) ("[A] 'wire communication' must involve a transfer of the human voice." (citing 18 U.S.C. § 2510(1))). A separate reason for saying that the "wire communication" definition does not apply is that cellular communications do not rely upon wires, cables, or like connections. *See* 18 U.S.C. § 2510(1) (defining "wire communication" to require "transmission . . . by the aid of wire[] [or] cable"). This reason possesses the added virtue of putting outside of the "wire communication" definition all cellular communications, not just CSLI itself.

186. *See Orenstein*, 396 F. Supp. 2d at 307 (rejecting the government's contention that it can compel disclosure of prospective CSLI pursuant to § 2703(d)); *Smith*, 396 F. Supp. 2d. at 759 (same).

> The most glaring difficulty in meshing these disparate statutory provisions is that with a single exception they do not cross-reference one another. The [PRS] does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the [PRS]; and the CALEA proviso does not mention the SCA. CALEA does refer to the [PRS], but only in the negative sense of disclaiming its applicability. Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way. This is especially so given that no other form of electronic surveillance has the mixed statutory parentage that prospective cell site data is claimed to have.[187]

Despite these compelling arguments against the hybrid theory, some courts accept the theory and allow the disclosure of real-time CSLI under the SCA's § 2703(d) standard.[188] These courts accept all three of the hybrid theory's premises. First, they believe that the post-PATRIOT Act definitions in the PRS, particularly by way of their inclusion of "signaling information," bring CSLI within the scope of the PRS.[189] They reject the argument that the PATRIOT Act did not intend CSLI to fall under the PRS by asserting that the clear language of the PRS precludes the need to look at legislative history.[190]

Courts that permit disclosure under the SCA standard also accept the hybrid theory's second premise:

> [T]he most natural reading of Section 1002(a)(2) [of the CALEA] is that [CSLI] may not be disclosed pursuant to the [PRS] alone without authorization by some other statutory provision. It follows that [CSLI] may be disclosed pursuant to the [PRS] *and* some additional statutory authority. In other words, Section 1002 does not prevent courts from authorizing the disclosure of [CSLI] under the [PRS]. It merely requires additional statutory authority for any such order.[191]

---

187. *Smith*, 396 F. Supp. 2d at 764–65.

188. *See supra* note 19 (noting that eight of twenty-eight decisions to address the proper standard for the disclosure of real-time CSLI have held that probable cause is not required).

189. *See, e.g.*, *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel. (Kaplan), 460 F. Supp. 2d 448, 455 (S.D.N.Y. 2006) ("The amended definitions encompass the cell site information the government seeks here.").

190. *See, e.g.*, *id.* at 456 (rejecting the view that the new PRS definitions were meant only to cover e-mail).

191. *Id.* at 457. *Accord In re* Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info. (Rosenthal), 622 F. Supp. 2d 411, 416–17 (S.D. Tex. 2007) (reading the CALEA to allow the PRS to be used with an additional statute).

These courts reject the view that § 1002(a)(2) should be read to prohibit the obtaining of location information through the PRS altogether, stating that such a reading would give no effect to Congress's inclusion of the word "solely."[192]

Finally, courts that accept the hybrid theory find that the SCA applies to CSLI and that the SCA therefore can provide the additional authority permitted by the CALEA.[193] Many of these courts assert that CSPs provide an "electronic communications service" without providing an explanation as to how CSPs fit within that definition.[194] These courts further claim that real-time CSLI can constitute "a record or other information pertaining to a subscriber," pointing out that CSLI is at least momentarily stored before it is turned over to law enforcement officials.[195] Proponents of the hybrid theory conclude their defense of the SCA's applicability by arguing that the "tracking device" exception either does not apply or, as one court declared, is irrelevant:

> Whether a cell phone is a tracking device . . . is immaterial to the precise question before the Court, which is whether the government is entitled to an order under Section 2703. That section . . . [covers] disclosure of "a record or other information pertaining to a subscriber to or a customer of an *electronic communications service*." It does not authorize the disclosure of an "*electronic communication*. . . ." For the tracking device exception to have force here, the Court would have to incorporate the term "electronic communication" into the term "electronic communications service."[196]

On the basis of their acceptance of the hybrid theory's three premises, courts that accept the theory conclude that the government can compel disclosure of real-time CSLI—through the combined use of the PRS and the SCA, as authorized by the CALEA—upon a showing of "specific and articulable facts" establishing that the CSLI being sought is "relevant and material to an ongoing

---

192. *See Rosenthal*, 622 F. Supp 2d at 417 (explaining that the opposite conclusion "gives effect to the 'solely pursuant' language in CALEA"); *Kaplan*, 460 F. Supp. 2d at 458 ("This interpretation . . . requires reading the word 'solely' out of the statute entirely . . . .").

193. *See Rosenthal*, 622 F. Supp 2d at 417 (accepting Judge Kaplan's conclusion that CSLI fits within the SCA); *Kaplan*, 460 F. Supp. 2d at 459–60 (explaining how CSLI fits within the framework of the SCA).

194. *See Rosenthal*, 622 F. Supp 2d at 417 (citing to Judge Kaplan and stating that courts have found CSPs to be providers of an "electronic communications service"); *Kaplan*, 460 F. Supp. 2d at 459 ("Cell phone service providers clearly fit within th[e] definition [of 'electronic communications service'].").

195. *See Kaplan*, 460 F. Supp. 2d at 459 ("The [SCA] contains no explicit limitation on the disclosure of prospective data. Further, the information the government requests is, in fact, a stored, historical record because it will be received by the [CSP] and stored, if only momentarily, before being forwarded to law enforcement officials.").

196. *Id.* at 460.

criminal investigation."[197] For the reasons set out above, this view has proven difficult to defend and has been widely rejected by courts.

IV. Historical CSLI: Arguments Surrounding the Proper Standard

A. Statutory Arguments

1. Applying the SCA Alone to Historical CSLI

As the previous section indicates, one of the reasons courts have rebuffed governmental efforts to obtain prospective CSLI is their unwillingness to apply the SCA—a statute governing disclosure of *stored* communications—to real-time information.[198] This problem seemingly is eliminated in the context of historical CSLI, which appears to fit much more comfortably within the SCA framework.[199] Although many courts—either expressly or in dicta—have relied on this logic to conclude that historical CSLI can be disclosed under the SCA's "specific and articulable facts" standard,[200] a closer look at the SCA calls this conclusion into question.

a. Applying the "Tracking Device" Definition

Because cellular communications, and thus CSLI, do not qualify as a form of "wire communication,"[201] the SCA applies to historical CSLI only if cellular communications can be classified as a form of "electronic communication."[202] The term "electronic communication" explicitly excludes "communication[s] from a tracking device,"[203] and "tracking device" is defined as "an electronic or

197. *See, e.g., id.* at 462 (concluding that the SCA's § 2703(d) standard governs the compelled disclosure of real-time CSLI).

198. *See supra* note 173 and accompanying text (discussing the unwillingness of courts to apply the SCA to real-time CSLI).

199. *See, e.g., In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) ("By contrast, historical cell site data more comfortably fits the category of transactional records covered by the SCA.").

200. *See supra* notes 21–22 and accompanying text (citing to cases that have held or stated in dicta that historical CSLI can be disclosed under the SCA standard).

201. *See supra* note 71 and accompanying text (illustrating why cellular communications, and thus CSLI, do not qualify as a form of "wire communication").

202. *See supra* note 56 and accompanying text (explaining that the scope of the SCA is limited to stored wire and electronic communications).

203. 18 U.S.C. § 2510(12)(C) (2006).

mechanical device which *permits* the tracking of the movement of a person or object."[204] Thus, the SCA does not allow for the disclosure of information gathered from devices that have tracking capabilities, at least when wire communications are not at issue.

Those who argue that probable cause—not § 2703(d) of the SCA—should govern the disclosure of historical CSLI note the striking breadth of the tracking device definition, focusing on the fact that the device need only "permit" tracking.[205] In light of the fact that cell phones allow for the discovery of their users' locations to within at least a few hundred feet, it seems beyond question that they are devices which "permit" tracking.[206] This conclusion does not change, proponents of probable cause assert, simply because the location information in question has been stored:

> [This] explanation is tantamount to an assertion that the *mere storage* of what appears indisputably to be information from a tracking device when garnered, alters its character. No such archival alchemy is possible. The frequent and specific information of our physical movements now transmitted by our cell phones is, necessarily, *and remains*, information from a device that permits the tracking of movement. The source of information does not change when it is stored.[207]

More importantly, if location information ceases to be a "communication from a tracking device" at the moment when it is stored, then the SCA, which governs only stored communications, has no need for its tracking device exclusion.[208] Because historical CSLI falls squarely within the tracking device definition, proponents of the probable cause standard argue, it necessarily falls outside the scope of the SCA.[209]

---

204. *Id.* § 3117(b) (emphasis added).

205. *See, e.g.*, *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. (Alexander I), 509 F. Supp. 2d 64, 74 (D. Mass. 2007) (describing the definition as "broad" and citing to other cases that have described it similarly), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007).

206. *See Lenihan*, 534 F. Supp. 2d 585, 602 (W.D. Pa. 2008) ("Even without triangulation, our cell phones transmit—and our CSPs record—information of our movements to a few hundred feet. It is, therefore, extremely difficult to see how a cell phone is not now *precisely* an 'electronic . . . device which permits the tracking of the movement of a person or object.'" (quoting 18 U.S.C. § 3117(b))).

207. *Id.* at 603.

208. *See id.* (concluding that the SCA's express exclusion of communications from tracking devices would be rendered superfluous if one accepts the view that such communications can no longer be considered "from tracking devices" once they are stored).

209. *See id.* at 601 (stating that historical CSLI is beyond the reach of the SCA because the tracking device definition means that historical CSLI is not an "electronic communication").

Those who believe that historical CSLI can be disclosed under the SCA standard, on the other hand, attempt to argue their way around the SCA's tracking device limitation. Judge Stearns, for instance, points out that the information allowed to be disclosed under § 2703(d) is significantly more detailed than the simple "transactional" data that can be disclosed under § 2703(c) by mere subpoena.[210] Because of this, he sees no problem with using § 2703(d) (the "specific and articulable facts" standard) to obtain detailed information such as CSLI.[211] Additionally, Judge Stearns argues that the tracking device limitation is of no consequence to § 2703(d): "[N]othing in the . . . definition of a mobile tracking device places a limitation on the 'records or other information' obtainable pursuant to a section 2703(d) order."[212]

On the question of whether the SCA's tracking device limitation applies, the arguments made by proponents of probable cause effectively undermine Judge Stearns's view. In short, Judge Stearns's contention on behalf of opponents of the probable cause standard misses the point; the tracking device definition need not expressly limit § 2703(d) because the SCA (which includes § 2703(d)) already disclaims its applicability to tracking devices.[213] Proponents of probable cause, therefore, are correct to find that CSLI falls outside the scope of the SCA.

b. Is Historical CSLI "Records or Other Information" Under § 2703(c)?

For historical CSLI to be disclosed under the SCA's § 2703(d) standard, it must qualify as "a record or other information pertaining to a subscriber to or customer of [an electronic communication] service."[214] Those who argue for the probable cause standard contend that historical CSLI falls outside of this category. They begin by restating their position that CSLI is excluded from the SCA's definition of "electronic communication" because it constitutes data

---

210. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 80 n.8 (D. Mass. 2007) ("[T]he 'records and other information' obtainable by means of a section 2703(d) order must consist of data containing greater detail than the records subject to an administrative subpoena by section 2703(c)(2).").

211. *See id.* (accepting the use of § 2703(d) to obtain relatively detailed communications data).

212. *Id.*

213. *See supra* note 56 (providing examples of provisions in the SCA that illustrate that the Act's scope is limited to wire and electronic communications); *supra* notes 73–74 and accompanying text (explaining that tracking devices are excluded from the SCA's definition of "electronic communication").

214. 18 U.S.C. § 2703(c) (2006).

from a "tracking device."[215] They then argue that the tracking device limitation is meaningless if "stored information from a tracking device nonetheless comes directly back—as a record pertaining to an electronic communication service—into the scope of the SCA."[216] In an attempt to reconcile the SCA's exclusion of tracking device information with its coverage of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication] service," proponents of probable cause advocate a narrow reading of § 2703(c):

> This court . . . read[s] the provision of § 2703(c) to authorize disclosure of records and other information *directly* pertaining to a subscriber/customer of an electronic communication service. That is, information that is regarding or derived under a service (*e.g.*, a tracking capability/function) that may be used to facilitate the provision of an electronic communication service (*e.g.*, the transmission of voice/text material), but that is not *itself* an electronic communication service (as, *e.g.*, by definition), does not "pertain" to the subscriber of an electronic communications service within the meaning of the statute.[217]

Those who oppose the application of probable cause to the disclosure of historical CSLI reject this interpretation of § 2703(c), arguing that it instead must be understood in light of the "ordinary usage" of its language.[218] Judge Stearns outlined this position: "In the relevant context, a record means something stored or archived. The term information is synonymous with data. [CSPs] store data gleaned from the cell towers through which telephone calls are routed. Thus, historical [CSLI] is a 'record or other information pertaining to' a customer . . . ."[219]

Although the ordinary usage approach has an obvious logical appeal, it possesses a fatal flaw that is not fleshed out by the proponents' arguments: It is premised upon the erroneous assumption that CSPs provide an "electronic communication service." In order for a service to constitute an "electronic communication service" under the SCA, it must "provide[] . . . users [with] the ability to send or receive wire or electronic communications."[220] Cellular

---

215. *See Lenihan*, 534 F. Supp. 2d 585, 604 (W.D. Pa. 2008) (describing CSLI as a communication from a "tracking device," as that term is defined statutorily).

216. *Id.*

217. *Id.*

218. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) ("Since neither the term 'record' nor the term 'information' is defined by the SCA, a court must look to the meaning of the terms in their ordinary usage.").

219. *Id.*

220. 18 U.S.C. § 2510(15) (2006).

telephone calls and text messages are not "wire communications" because they are not made through wires, cables, or similar connections,[221] and are not "electronic communications" because they derive from devices that "permit the tracking of the movement of a person or object."[222] Accordingly, CSPs do not provide an "electronic communication service" within the meaning of the SCA. The "ordinary usage" approach applied by opponents of the probable cause standard, therefore, fails to place its interpretation within the context of the statute as a whole. When that context is taken into account, it becomes clear that historical CSLI cannot be classified as "a record or other information pertaining to a subscriber to or customer of [an electronic communication] service."

2. Revisiting the Hybrid Theory

As discussed above, courts have widely rejected the government's hybrid theory in the context of applications for real-time CSLI.[223] The question remains, at least to some, whether the hybrid theory is still alive in the historical CSLI context. Courts that feel that the question is closed—those that require probable cause for the disclosure of historical CSLI—simply argue that the rationales for rejecting the hybrid theory with respect to real-time CSLI apply with equal force to historical CSLI.[224] This view is compelling given that the arguments against the hybrid theory are not specific to prospective CSLI, but are attacks on the logic of the theory itself. Although some courts that have allowed disclosure of historical CSLI under the § 2703(d) standard have avoided the hybrid theory and reached their decisions through the SCA alone,[225] at least one court has compelled disclosure of historical CSLI using

---

221. *See id.* § 2510(1) (defining the term "wire communication" to require "transmission . . . by the aid of wire, cable, or other like connection").

222. *See id.* § 2510(12)(C) (excluding "communication[s] from [] tracking device[s]" from the definition of "electronic communication"); *see also id.* § 3117(b) (defining the term "tracking device"). For a fuller discussion of how the "tracking device" limitation applies to historical CSLI, see *supra* Part IV.A.1.a.

223. *See supra* Part III.C (discussing the hybrid theory and its rejection by a significant majority of courts).

224. *See Lenihan*, 534 F. Supp. 2d 585, 609 (W.D. Pa. 2008) (declaring with respect to the hybrid theory that the court "need not tarry on this widely—and rightly—refuted contention"); *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. (Alexander I), 509 F. Supp. 2d 64, 72 (D. Mass. 2007) ("This 'hybrid' approach has, however, largely been rejected as contrary to Congress'[s] intentions."), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007).

225. *See, e.g.*, *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code,

the hybrid theory.[226] Nevertheless, this court's acceptance of the theory was conclusory and devoid of analysis. After laying out the familiar hybrid theory logic, it declared:

> Both historical and prospective cell-site data are "a record or other information pertaining to a subscriber to or customer of" an electronic communication service. Under this approach, the Government may obtain certain cell-site information under the [PRS] and the [SCA] if, as here, it makes the showing required under both statutes.[227]

Given the many valid reasons for rejecting the hybrid theory with respect to *all types* of CSLI, as well as the lack of any substantive reason for responding to these criticisms and accepting the theory in the historical CSLI context, it seems safe to say that the hybrid theory has no place in historical CSLI jurisprudence.

3. Understanding the CALEA and Its Legislative History

Another contentious point in CSLI literature and jurisprudence is how courts should understand the CALEA's limitation on the disclosure of location information and the legislative history that gave rise to that limitation. Proponents of applying probable cause to historical CSLI rely heavily on the legislative history of the CALEA, noting that its passage was dependent upon assurances from the FBI that the CALEA would not change the then-existing requirements for obtaining location information.[228] Thus, they assert that the CALEA constitutes Congress's clear intent to prevent disclosure of location information except under the traditional standard that governs disclosure, namely probable cause: "With CALEA, which specifically and unequivocally prohibits the Government's use of the [PRS] to enable its commandeering of an unsuspecting user's cell phone as a tracking device, Congress clearly

---

Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (finding that because historical CSLI is a "record or other information pertaining to a subscriber to or customer of" an electronic communication service it can be disclosed under the SCA's § 2703(d) standard).

226. *See In re* Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info. (Rosenthal), 622 F. Supp. 2d 411, 417 (S.D. Tex. 2007) (permitting the disclosure of both historical and prospective CSLI under the combined authority of the PRS and SCA, thereby accepting the hybrid theory).

227. *Id.* (citations omitted).

228. *See Lenihan*, 534 F. Supp. 2d at 596–97 (discussing FBI Director Louis Freeh's testimony before Congress on the CALEA as well as its implications for CSLI disclosure).

demonstrated its intent to prevent the tracking of individuals without a probable cause determination."[229]

Those who oppose a probable cause standard for historical CSLI reject this characterization of the CALEA and its legislative history, instead looking more closely at the context in which FBI Director Freeh's comments were made. They point out that at the time Freeh made his comments in 1994, "pen/trap devices, as statutorily defined [in the PRS] in 1986, were . . . incapable of determining cell phone locations," and the use of computers to store CSLI "was a somewhat distant, if not unimagined vision—especially for law enforcement investigative uses."[230] They further note that Director Freeh, in acknowledging that cellular carriers compiled location information at that time, dismissed concern over such data, saying that it merely was used for business purposes and that it did not raise the risk of "true tracking."[231] Because "true tracking" referred to surveillance of the sort that took place in *Knotts* and required probable cause, opponents of probable cause contend that Director Freeh's testimony rejected the view that CSLI can be disclosed only upon a showing of probable cause.[232] Opponents additionally argue that Freeh was concerned with limiting disclosure of "call setup information" rather than data related to business purposes, the latter of which he thought included CSLI.[233] Accordingly, opponents of probable cause conclude that Director Freeh—and therefore Congress, in enacting the CALEA—did not mean to bring CSLI within the CALEA's limitation upon the disclosure of location information.[234]

Although the argument made by opponents of probable cause has some validity, there is a basis for rejecting it that is independent from the basis put forth by proponents of probable cause. It is true that at the time, Director Freeh could not have known that the PRS subsequently would come to cover processes such as the storage of CSLI. Nevertheless, Congress subsequently expanded the scope of the PRS apparently to include CSLI without making any

---

229. *Alexander I*, 509 F. Supp. 2d at 74.

230. Clark, *supra* note 8, at 1463.

231. *See id.* ("Director Freeh conceived of cell phone location information as data only for business . . . and not, in his words, for the sort of 'true tracking' engaged in by law enforcement for criminal investigative purposes.").

232. *See id.* at 1463–64 (describing the notion of "true tracking" and noting that Freeh was aware of its meaning and the various disclosure tools available to law enforcement).

233. *See id.* at 1464 (distinguishing between "call setup information," with which Freeh was concerned, and "transactional" data relating to business, with which he was not concerned).

234. *See id.* at 1463–65 (analyzing Freeh's testimony before Congress and concluding that CSLI was not intended to be affected by the "location information" limitation in the CALEA).

corresponding changes to the CALEA.[235] The necessary conclusion to be drawn from this course of action is that the *present* intent of Congress with respect to the CALEA is to prevent the PRS—as it now exists—from being used to compel disclosure of "information that may disclose the physical location of the subscriber."[236] Because CSLI discloses the physical location of a subscriber, it currently falls within the CALEA limitation—regardless of what Director Freeh and Congress may have intended or foreseen in 1994.

B. Fourth Amendment Jurisprudential Arguments

1. Is the Fourth Amendment Even Implicated?

The question of whether the Fourth Amendment applies to the disclosure of historical CSLI depends upon whether such disclosure constitutes a "search" for purposes of the Amendment.[237] Under Justice Harlan's classic formulation, a search occurs when an individual manifests an actual (subjective) expectation of privacy and when that expectation is one that society is prepared to accept as reasonable.[238] The application of this definition to historical CSLI breeds a corresponding two-part inquiry: (1) whether cell phone users can manifest an actual expectation that their stored location information will remain private; and (2) whether, if so, society would find this expectation to be reasonable. Proponents of the probable cause standard argue that each of these questions can be answered in the affirmative,[239] while opponents attack both prongs, thereby claiming that the Fourth Amendment is not even implicated by the disclosure of historical CSLI.[240]

Proponents of the probable cause standard assert that cell phone users maintain a subjective expectation of privacy in historical records of their

---

235. *See supra* notes 153–55 and accompanying text (discussing the PATRIOT Act's expansion of the PRS and the government's contention that the PRS now covers CSLI).

236. 47 U.S.C. § 1002(a)(2) (2000).

237. *See supra* note 92 and accompanying text (noting that the Fourth Amendment is not implicated unless a governmental action constitutes either a "search" or a "seizure").

238. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (defining the term "search" to require both a subjective and objective (reasonable) expectation of privacy).

239. *See infra* notes 241–42, 244–47, 249–51 and accompanying text (explaining the reasons why proponents of probable cause for historical CSLI believe that individuals maintain subjective and reasonable expectations of privacy in such data).

240. *See infra* notes 243, 248 and accompanying text (noting the argument of opponents of probable cause that individuals maintain neither subjective nor reasonable expectations of privacy in historical CSLI).

movements because most do not even know that such records can be created.[241] Judge Lenihan summarized this position:

> The Court believes, based on common experience within the community: First, that Americans do not generally know that a record of their whereabouts is being created whenever they travel about with their cell phones, or that such record is likely maintained by their cell phone providers and is potentially subject to review by interested Government officials. And second, that most Americans would be appalled by the notion that the Government could obtain such a record without at least a neutral, judicial determination of probable cause.[242]

Opponents of probable cause—those who assert that historical CSLI can be disclosed under the lesser SCA standard—contend that the assumption of the risk and tracking beeper cases preclude a finding that individuals can have a subjective expectation of privacy in stored CSLI.[243]

Those who argue that probable cause should govern the disclosure of historical CSLI also assert that the expectation of privacy in such data is one that society is prepared to accept as reasonable.[244] First, they rely on the aforementioned view that society would find appalling the idea that the government could surreptitiously track their movements without a judicial finding of probable cause.[245] They also believe that the expectation of privacy in historical CSLI is reasonable "because the [use of such] newly-emergent technologies create[s] a potential to monitor associational activities in a manner that could have a chilling effect," which is a result that society would not wish to condone.[246] Finally, proponents of probable cause contend that "the very fact that Congress has taken pains to protect electronically-derived location

---

241. *See Lenihan*, 534 F. Supp. 2d 585, 611 (W.D. Pa. 2008) (finding that Americans possess a subjective expectation of privacy in their past movements recorded by the storage of CSLI).

242. *Id.*

243. *See, e.g.*, *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 81 (D. Mass. 2007) (finding that historical CSLI is governed by *Knotts* and that, therefore, no subjective expectation of privacy is implicated by attempting to prevent its disclosure); Clark, *supra* note 8, at 1470–71 (arguing that the assumption of the risk doctrine bars a finding of a subjective expectation of privacy in CSLI). For a discussion of the application of the assumption of the risk and tracking beeper cases in the historical CSLI context, see *infra* Parts IV.B.2–3.

244. *See, e.g.*, *Lenihan*, 534 F. Supp. 2d at 612 ("The Court further finds that the expectation of privacy in movement/location information . . . is objectively reasonable . . . .").

245. *See id.* at 611 ("[M]ost Americans would be appalled by the notion that the Government could obtain [CSLI] without at least a neutral, judicial determination of probable cause.").

246. *Id.* at 612.

information from unwarranted disclosure [in the CALEA and § 3117(b)] serves independently to make subjectively-held expectations of privacy objectively reasonable."[247] Opponents of probable cause again point to the assumption of the risk and tracking beeper cases, arguing that these lines of jurisprudence preclude a finding that subjectively held expectations of privacy in historical CSLI are reasonable.[248]

Proponents of probable cause extend their argument one step further, contending that past expectations of privacy remain reasonable even after the events giving rise to those expectations have come to pass.[249] Specifically, they point out that an individual's legitimate expectation of privacy in the fact that she was going to travel to a certain location (or was then present at a location) does not vanish after she travels to and then leaves that location.[250] In other words, if an individual wishes not to disclose information about the destinations to which she *will be traveling*, that individual maintains a privacy interest in guarding against disclosure of those destinations *even after having gone to and left them*. Judge Alexander explained this point: "It would be nonsensical to think that revelation of a location that [one] wished to keep secret up to and during his attendance would suddenly become appropriate simply because the activity is over and he has left the location."[251] This argument defends against the claim that individuals lose the expectation of privacy they may have in their locations and movements, recorded in real-time by CSLI, once those movements, and thus the CSLI, can be classified as "historical."

2. *Assumption of the Risk*

In *United States v. Miller* and *Smith v. Maryland*, the Supreme Court ruled that individuals possess no legitimate expectation of privacy in information they voluntarily convey to third parties—a doctrine referred to as "assumption of the

247. *Id.*

248. *See supra* note 243 (citing reliance on both assumption of the risk and the tracking beeper cases to find that there is no legitimate expectation of privacy in CSLI).

249. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. (Alexander I), 509 F. Supp. 2d 64, 74–75 (D. Mass. 2007) (arguing that individuals who hold an expectation of privacy in their location do not lose that expectation upon leaving that location), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007).

250. *See id.* ("Expecting a right to privacy in the location of where one is, or where one will be shortly, yet losing that expectation once leaving a location, is nonsensical.").

251. *Id.* at 75.

risk."[252] Particularly relevant to the CSLI discussion is *Smith*, in which the Court held that individuals possess neither a subjective nor a reasonable expectation of privacy in the telephone numbers they dial.[253] As the prior section indicates, the application of this doctrine is crucial, as a finding of assumption of the risk with respect to CSLI means that the Fourth Amendment does not apply to its disclosure.[254]

Proponents of the probable cause standard for historical CSLI argue that the assumption of the risk analogy is inapposite because CSLI is not information that users convey *voluntarily*.[255] To the contrary, CSLI is generated through a process that occurs automatically every seven seconds when a user's cell phone is turned on and that requires no action on the part of the user.[256] Because CSLI is conveyed without user intervention, proponents of probable cause contend that the assumption of the risk doctrine—which depends upon individuals voluntarily conveying information—simply does not apply.[257]

Opponents of the probable cause standard disagree, arguing that CSLI squarely falls within the doctrine. They assert that even with the automatic nature of the registration process, cell phone users voluntarily convey CSLI because they voluntarily choose to use cell phones:

> Just as no one forces a bank customer to do business with a financial institution, no one forces a target to use a cell phone. It is the user's conscious decision to activate and operate the instrument and s/he "assumes the risk" that the service provider will turn over to law enforcement the location information that the user broadcasts while carrying about a cell phone in operation.[258]

---

252. *See supra* Part III.B.2 (summarizing *Miller* and *Smith* and their application of the assumption of the risk doctrine).

253. *See supra* notes 110–13 and accompanying text (describing the *Smith* Court's reasons for rejecting the defendant's Fourth Amendment claim).

254. *See supra* notes 243, 248 and accompanying text (noting that opponents of the probable cause standard for historical CSLI argue that there can be neither subjective nor reasonable expectations of privacy in historical CSLI due to assumption of the risk).

255. *See Lenihan*, 534 F. Supp. 2d 585, 614–15 (W.D. Pa. 2008) (arguing that assumption of the risk does not apply to historical CSLI); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005) (arguing that assumption of the risk does not apply to prospective CSLI).

256. *See supra* notes 34–35 and accompanying text (describing the process of "registration").

257. *See, e.g.*, *Smith*, 396 F. Supp. 2d at 756 ("Unlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. . . . [I]t is transmitted automatically during the registration process, entirely independent of the user's input . . . .").

258. Clark, *supra* note 8, at 1470–71.

Although this argument facially rebuts the claim made by proponents of probable cause, it ignores the fact that in today's world, the "choice" to use a cellular telephone is really no choice at all.[259] The opponents of probable cause grossly understate the extent to which cellular communications have become a necessity in our society. Although many individuals choose to have cell phones for personal reasons, hoards of others are required to carry them for work, business, and other legitimate purposes. In light of such varying motivations for using cellular devices, it is inaccurate to proclaim that all cell phone users are truly "voluntary" users.

More importantly, one's voluntary decision to use a cell phone cannot be equated with a voluntary choice *to convey CSLI*, as CSLI is an automatic byproduct of cell phone use of which the average user is unaware.[260] Individuals using cell phones, in other words, do not make an informed choice to allow their providers to record information about their movements. It is no argument to say that users remain free to turn their phones off: "[F]rom a practical standpoint the option to turn the phone off hardly seems like an option, as it strips the phone of its ability to receive calls."[261] Like the argument that users may choose not to have cell phones in the first place, "[p]rotecting oneself by not using the phone simply fails to recognize the reality of cell phone usage in modern life."[262]

3. The Tracking Beeper Cases

Through its decisions in *United States v. Knotts* and *United States v. Karo*, the Supreme Court established that the use of a tracking device by law enforcement officials constitutes a search under the Fourth Amendment when the device is used to track an individual's private movements, but not when it is used only to ascertain a person's publicly-visible movements.[263] In light of this distinction, those who assert that probable cause governs the disclosure of historical CSLI contend that CSLI has the potential to implicate private

259. *See* McLaughlin, *supra* note 4, at 441 (stating that the argument that people can choose not to use cell phones "fails to recognize the reality of cell phone usage in modern life").

260. *See supra* notes 241–42 and accompanying text (discussing Judge Lenihan's conclusion that the public generally is unaware of the tracking capabilities of cellular phones). *Accord* McLaughlin, *supra* note 4, at 439 ("Many Americans may be unaware today that their location can be tracked with their cell phones . . . .").

261. McLaughlin, *supra* note 4, at 436.

262. *Id.* at 441.

263. *See supra* notes 146–48 and accompanying text (summarizing the Fourth Amendment implications of *Knotts* and *Karo*, when taken together).

movements (as in *Karo*),[264] while opponents respond that CSLI is analogous to the public movements at issue in *Knotts*.[265] As with assumption of the risk, the application of the *Knotts/Karo* distinction to historical CSLI is essential to determining whether the Fourth Amendment even applies to its disclosure.[266]

Proponents of the probable cause standard contend that historical CSLI falls under *Karo* rather than *Knotts* because courts disclosing such data will never be able to ensure that it reveals only the user's location and movements *in public*.[267] Because the practical reality is that CSPs are unable to filter their CSLI according to the type of location it reveals,[268] orders to disclose CSLI will "almost certainly result in over-inclusive disclosures, and thus in transgressions of Constitutional boundaries."[269] When the government is uncertain as to whether its actions will invade spheres of privacy protected by *Karo*—an uncertainty that it always has with respect to CSLI—its only option to avoid a constitutional violation is to obtain a warrant supported by probable cause.[270] In so doing, the government cannot be heard to complain that this standard would impose upon it too great a hardship, as the Supreme Court has proclaimed that "[t]he argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement."[271]

Opponents of the probable cause standard for historical CSLI argue that there is no danger that CSLI can reveal an individual's private movements in the sense prohibited by *Karo*. This argument was spelled out by Judge Stearns:

---

264. *See infra* notes 267–71 and accompanying text (presenting the arguments raised by proponents of probable cause with respect to applying the tracking beeper cases to the disclosure of historical CSLI).

265. *See infra* note 272 and accompanying text (presenting the argument raised by opponents of probable cause with respect to applying the tracking beeper cases to the disclosure of historical CSLI).

266. *See supra* notes 243, 248 and accompanying text (noting that opponents of the probable cause standard for historical CSLI argue that there can be neither subjective nor reasonable expectations of privacy in historical CSLI due to the application of the tracking beeper cases).

267. *See Lenihan*, 534 F. Supp. 2d 585, 613 (W.D. Pa. 2008) (finding that orders granting disclosure to CSLI "would almost certainly result in over-inclusive disclosures" under *Karo*).

268. *See id.* (suggesting that CSPs cannot filter CSLI based on location).

269. *Id.*

270. *See In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) ("Because the government cannot demonstrate that [CSLI] could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat [CSLI] differently from other forms of tracking . . . which routinely require probable cause.").

271. United States v. Karo, 468 U.S. 705, 718 (1984).

"The most that the 'tracked' cell phone might reveal is that its owner might presently be found in the home . . . . There is nothing, however, about that disclosure that is any more incriminating or revealing than what could be gleaned from . . . physical surveillance."[272] Put differently, the argument is that historical CSLI falls under *Knotts*; it is information that conveys no more to law enforcement than what they could have seen had they followed the individual's public movements.

The problem with the view that historical CSLI is akin to the information at issue in *Knotts*—a problem that is hinted at but not discussed by the proponents of probable cause—is that it rests upon an unfounded confidence in the imprecision of CSLI. In making their argument, opponents of the probable cause standard implicitly assert that CSLI can *never* reveal an individual's movements in places shielded from public view, for if it was possible that CSLI could reveal such information, probable cause would be required to satisfy *Karo*.[273] The problem arises from the fact that CSLI—including historical CSLI—is capable of determining a user's location to within a few hundred feet and, in some cases, to within an even smaller radius.[274] It simply is incorrect to say that a device that pinpoints a person's location to within a few hundred feet (or closer) never can reveal that the person has changed her location while remaining shielded from visual surveillance. One need only consider a cell phone user who, carrying her phone, moves from one end of her palatial private residence to another; in such a case, CSLI would allow officers to learn about that user's wholly private movements in a way offensive to *Karo*. Although examples involving sprawling but private locations of this sort admittedly are exceptional cases, even exceptional cases undermine the opponents' position that CSLI *never* can reveal more than that which can be observed by visual surveillance.

V. Proposed Solution: A Call to Congress

Underlying the entire debate regarding the proper standard for the disclosure of CSLI is the elephant in the room: Congress's ongoing failure to clear up this particularly messy area of the law. Although the statutes as they

---

272. *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) (Stearns), 509 F. Supp. 2d 76, 81 (D. Mass. 2007).

273. *See Karo*, 468 U.S. at 714 (finding that a warrant is required to track an individual in "a location not open to visual surveillance").

274. *See supra* notes 46–47 and accompanying text (describing the level of precision with which CSLI reveals users' locations).

currently stand resolve this question in favor of probable cause, the contentiousness of the debate and the continuing occurrence of reported cases on the issue indicate that additional clarity is sorely needed. The government's "hybrid" approach of piecing together cherry-picked portions of electronic surveillance law serves as further evidence that the current statutory structure is convoluted.

Congressional action provides the only course through which this question can escape the labyrinth of caselaw and be resolved definitively. The issue of what showing is required before courts may disclose users' CSLI can no longer be written off as a novel problem that Congress has not had time to investigate and address. The time has come for Congress to provide specific legislation that governs and makes uniform the issuance of court orders compelling the disclosure of CSLI.

As the previous section argues, the only way that a law can permit the disclosure of CSLI while complying with the privacy boundaries established under the Fourth Amendment is for it to require probable cause as to *both* real-time and historical CSLI. Congress could opt to impose this probable cause requirement through amendment of the current statutes: the SCA, the PRS, and the CALEA. A much clearer and more effective approach, however, would be to enact a brief but separate piece of legislation directly addressing court-ordered CSLI disclosure. This course of action would make Congress's intent significantly less equivocal. The following model provision would properly address the issuance of court orders for CSLI:

> (a) A court shall not grant a Government application to compel disclosure of cell site location information, whether real-time or historical, and shall not otherwise order disclosure of such information, except upon a showing of probable cause as authorized by Rule 41 of the Federal Rules of Criminal Procedure.
>
> (b) This law shall serve as the sole authority upon which a court may order disclosure of real-time and/or historical cell site location information.

Enacting this specific provision would eliminate the two problems that have plagued CSLI jurisprudence to date: the tortuous application of a series of separate statutes and, more importantly, the failure of courts uniformly to impose a requirement of probable cause.

VI. Conclusion

Because courts so frequently have thwarted law enforcement attempts to obtain real-time CSLI at a less than probable cause standard,[275] it seems likely that efforts to obtain historical CSLI will be on the rise in the coming years. Although the government contends that there is a statutory basis for permitting courts to compel the disclosure of historical CSLI at a reduced standard, a close examination of this argument proves that it does not hold up to the rigors of the statutes' application.[276] More importantly, an interpretation of the applicable electronic surveillance statutes that would allow historical CSLI to be disclosed at a less than probable cause standard raises the specter of inevitable Fourth Amendment violations.[277] Given the absence of statutory authority for imposing a lesser standard and the overriding Fourth Amendment default requirement of probable cause, there is no basis for permitting the disclosure of historical CSLI upon any showing less than probable cause.

Ultimately, requiring the government to establish probable cause to compel the disclosure of historical cell site location information strikes the appropriate balance between law enforcement objectives and the vital privacy interests of American cell phone users. This was the balance reached by Judge Smith, whose well-articulated conclusion was echoed by Judge Lenihan at the close of her landmark historical CSLI decision:

> Denial of the government's request for . . . cell site data . . . should have no dire consequences for law enforcement. This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected. Absent any sign that Congress has squarely addressed and resolved those concerns in favor of law enforcement, the far more prudent course is to avoid an interpretation which risks a constitutional collision.[278]

---

275. *See supra* Part III.C (discussing courts' widespread rejection of the hybrid theory with respect to applications for real-time CSLI).

276. *See supra* Part IV.A (analyzing and rejecting the statutory arguments for disclosing CSLI under the SCA's "specific and articulable facts" standard).

277. *See supra* Part IV.B (applying relevant Fourth Amendment principles to the disclosure of historical CSLI and concluding that such disclosure constitutes a "search," thereby requiring the government to show probable cause).

278. *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith), 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (citations omitted).

When the disclosure of historical CSLI is at issue, there is only one way to avert such an inevitable constitutional collision: Imposing a requirement of probable cause. The time has come for Congress to make this clear.