University of Baltimore Law Review

Volume 42
Issue 3 *Spring 2013*

Article 5

2013

Location, Location, Location: Balancing Crime Fighting Needs and Privacy Rights

Nancy K. Oliver
Criminal Division, U.S. Department of Justice

LOCATION, LOCATION, LOCATION: BALANCING CRIME FIGHTING NEEDS AND PRIVACY RIGHTS

By Nancy K. Oliver*

I. INTRODUCTION

Rapid technological developments over the last twenty-five years have made cellular telephone location information ubiquitous and increasingly more detailed.[1] As a result, these developments have outpaced federal legislative solutions needed to address privacy concerns, on the one hand, and clarify standards for law enforcement access to such information, on the other.[2] At the same time, federal courts from coast to coast have sought to apply appropriate legal standards governed by these existing outdated statutory schemes and Fourth Amendment rights in determining law enforcement's access to information critical for criminal investigations and the fight against violent crime.[3] To further complicate the issues, as the technology has developed, the location information at issue before the courts has ranged from marginally accurate geographic historical data, to that which is real time and highly accurate, to within feet of the specific device's location.[4] Moreover, the accuracy of the information varies with the service provider and the cellular device.[5] The resulting jurisprudence is, by necessity, a hodgepodge.

---

* Trial Attorney, United States Department of Justice, Criminal Division, 1997-2008, Division Counsel, United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives, Baltimore Field Division, 2008-Spring 2013. Washington College of Law, The American University, J.D., University of Houston, B.A. Any opinions or points of view expressed in this article represent those of the author and do not necessarily represent the official position or policies of the United States Department of Justice. I would like to thank the hardworking agents at ATF and my other talented and dedicated DOJ colleagues for reminding me why I became an attorney, and I would especially like to thank Robert S. Carpenter for encouraging me to become one.

1. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 18–19 (2010) [hereinafter *ECPA Hearing*] (statement of Matt Blaze, Assoc. Professor, University of Pennsylvania).
2. *Id.* at 65–66 (statement of Mark J. Zwillinger, Zwillinger Genetski, LLP).
3. *Id.*
4. *Id.* at 14 (statement of Blaze).
5. *Id.* at 29–30.

Yet, just as technology evolves, so does the criminal element's sophistication in utilizing it to evade detection by law enforcement. For example, drug trafficking organizations have replaced a key resource, the beepers and pagers of the past, with the cell phones of today.[6] And more recently, readily available prepaid cell phones add the layer of anonymity to the criminal's essential tool for facilitating his crimes.[7]

Courts and Congress alike, along with scholars and privacy groups, have realized the need for legislative solutions to diverse issues raised by this advancing technology.[8] Although some courts and scholars have concluded that real-time location data should only be accessible on a showing of probable cause, that conclusion has only led to the need for a definition of "probable cause" in the context of obtaining location information.[9] However, the call for a probable cause standard for obtaining accurate, real-time location information requires further debate in the context of law enforcement investigative realities rather than merely assumed as a reactionary, prophylactic measure driven by Orwellian fears.

---

6. *See* Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV. 233, 254 (2010).

7. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 775 (3d Cir. 2012) (describing drug trafficking organization's use of prepaid phones); Lewis Medlock, *Prepaid Cell Phones: The New Growth Industry*, EZINE ARTICLES, http://ezinearticles.com/?Prepaid-Cell-Phones:-The-New-Growth-Industry&id=6192322 (last visited May 31, 2013) (describing growth in prepaid cell phones); Edward Lane, *Texas Senator Cornyn Proposes Law to Register Prepaid Cell Phones to Fight Criminals*, THE EXAMINER (June 7, 2010), http://www.examiner.com/article/texas-senator-cornyn-proposes-law-to-register-prepaid-cell-phones-to-fight-criminals (discussing Senator Cornyn's efforts to require registration of prepaid cell phones).

8. *See infra* notes 154–55 and accompanying text (discussing the meaning of probable cause and the potential issues of "retroactive unconstitutionality" raised by the "mosaic" theory); *see, e.g.*, *In re* United States for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone, 849 F. Supp. 2d 526, 553–56 [hereinafter *Gauvey Order*] (discussing the explosion of articles on cell site tracking by law enforcement, congressional hearings, and legislative proposals). Due to the long and cumbersome nature of the titles of cases dealing with applications for CSLI as well as the fact that they are all titled virtually the same, the author will take a cue from Magistrate Judge Austin from the Western District of Texas and use the following shorthand form to refer to the decisions in those cases: "[Judge] Order" followed by the citation to the reporting service.

9. *See infra* notes 125–32 and accompanying text.

II. A SHORT PRIMER ON CELL PHONE LOCATION INFORMATION

As any "smart" phone owner[10] is well aware, location information is integral to many, if not most, cell phones and the various applications users install on them to enhance their day-to-day lives. Facebook and Foursquare "friends" can let each other know their exact location at any given moment, while other applications inform users of dining, shopping, and entertainment opportunities nearby.[11] Before the explosion of cell phones and call forwarding technology an individual's phone number, by definition, told a caller the person's location when the call was answered. Today, a call may rouse our friend or colleague on the other side of the globe.

Unlike conventional land or wire-line telephones, cellular phones use radio waves to communicate with the cellular service providers' network of radio base stations.[12] The radio base station or tower communicates with the cell phone whenever a call is placed or received, as well as periodically when the cell phone automatically signals or identifies itself to the base station.[13]

With regard to cell phone location information, two different technologies are relevant. First, the cell phone handset may contain global positioning system (GPS) hardware that determines the cell phone's location—latitude and longitude—based on the phone's communication with satellites.[14] GPS location information calculated by the phone's handset, however, may or may not be sent to the cellular network or another third party, and is only reliable when the handset is outdoors and can "see" the GPS satellites.[15] Furthermore, the cellular service provider does not require GPS information to provide the cell phone service.[16]

The second type of technology, "network-based" location technology, does not depend on satellites or GPS technology and is

10. As of February 2012, 50% of American adults own a smart phone. *Smartphones Account for Half of all Mobile Phones, Dominate New Phone Purchases in the US*, NIELSEN WIRE (Mar. 29, 2012), http://www.nielsen.com/us/en/newswire/2012/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us.html.
11. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 708 (2011).
12. *ECPA Hearing*, *supra* note 1, at 20 (statement of Blaze).
13. *Id.*
14. *Id.* at 21.
15. *Id.* at 22.
16. *Id.* at 14.

based on information collected and analyzed by the cell phone providers' base stations.[17] As noted above, the user's cell handset uses radio waves to communicate with the base stations whenever making or receiving a call, as well as when it registers or identifies itself to the base station as it moves geographically throughout the system. Technically, the radio base stations, also known as "cell sites," are generally located on a cell "tower."[18] However, base stations are no longer limited to the tall three-sided radio towers commonly seen along the roadways; they may be mounted indoors as well and may be as small as a conventional stereo speaker.[19]

In order to route incoming or outgoing calls, the cellular network must keep track of the sector in which the phone is located.[20] The accuracy of the location information varies based on a number of factors, but generally becomes more accurate with the increasing geographic density of the towers and their cell sites and the corresponding decrease in the actual geographic area serviced by any particular cell site, i.e., the decreasing size of the cell sector.[21] According to the Cellular Telecommunications Industry Association, the number of cell sites has more than doubled between June 2002 and June 2012.[22]

In addition to decreasing cell site size, other technology available to cellular providers can pinpoint a phone's latitude and longitude within fifty meters or less by correlating the time and angle of arrival of the handset's signal as it moves to the different cell sites, regardless of whether calls are made or received as long as the phone is turned on.[23] Although the capabilities and retention practices of carriers vary, as noted by Professor Blaze in his testimony during Electronic Communications Privacy Act reform hearings, detailed location data provides valuable information to the carriers, and the trend of cellular providers to collect and maintain detailed location

17. *Id.* at 23.

18. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Should Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012).

19. *In re* United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S. D. Tex. 2010).

20. *ECPA Hearing*, *supra* note 1, at 14 (testimony of Blaze).

21. *Id.* at 23–24.

22. *50 Wireless Quick Facts*, CELLULAR TELECOMM. INDUST. ASS'N, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited May 31, 2013).

23. *ECPA Hearing*, *supra* note 1, at 26 (statement of Blaze).

records can be expected to continue as the technology needed to do so continues to develop. [24]

Location information can be generally categorized into 3 basic types: (1) information routinely collected by the cellular provider;[25] (2) information collected by the cellular provider upon request by law enforcement;[26] and (3) information that law enforcement collects independently of the cellular provider.[27] At a minimum, cellular service providers record and retain cell site location information (CSLI) in the regular course of their business when a call is placed or received.[28] The information is available on a historical as well as prospective or real-time basis. However, the terms "historical" and "prospective" can be ambiguous.[29] Historical CSLI refers to information recorded and stored by the service provider prior to the issuance of a court order.[30] The terms "prospective" and "real-time" are not synonymous, although they are frequently used interchangeably.[31] Real-time CSLI is that which the government uses to identify the location of the device at the moment it is transmitted and is a subset of prospective information, which is created anytime after the date of the court order.[32]

In addition to obtaining the CSLI for a particular cell number, a cellular provider can also provide all the cellular numbers and subscriber information recorded by a particular cell site or tower during a given time frame.[33]

---

24. *Id.* at 27–28. Location data is useful in identifying network deficiencies, redundancies, and customer usage, as well as marketing and developing new services; "service providers record everything essentially forever." *Id.* at 16.
25. *Id.* at 57 (testimony of Richard Littlehale, Assistant Special Agent, Tenn. Bureau of Investigation).
26. *See id.*
27. *See id.* at 57–58.
28. United States v. Jones, No. 05-0386, 2012 WL 6443136, at *2 (D. D.C. Dec. 14, 2012).
29. *ECPA Hearing*, *supra* note 1, at 86 (testimony of Stephen Smith, United States Magistrate Judge).
30. *In re* United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. On Tel. Numbers, 402 F. Supp. 2d 597, 599 (D. Md. 2005).
31. *ECPA Hearing*, *supra* note 1, at 86 (testimony of Smith) (citing *In re* United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. On Tel. Numbers, 402 F. Supp 2d 597, 599 & n.5 (D. Md. 2005)).
32. *Id.*
33. *See, e.g.*, *In re* The United States for an Order Pursuant to 18 U.S.C. § 2703(d), Nos. C-12-670M, C-12-671M, C-12-672M, C-12-673M, 2012 WL 4717778, at *1 (S.D. Tex. Sept. 26, 2012) [hereinafter *Owsley Order*].

The collection of more accurate location data based on the arrival of the handset's radio signals is available prospectively during a 911 call[34] and may be available to law enforcement when the carrier is asked to collect it.[35] Nevertheless, there is a growing trend for cellular providers to collect and maintain more accurate location information for their own purposes. Further, and most intrusively, law enforcement can use investigative tools that force a cell phone to send a registration signal to the investigative device and thereby identify the cell sector in which the phone is located.[36]

The foregoing discussion demonstrates that technology providing precise cell phone location information has changed dramatically and is likely to continue to do so. In addition, the accuracy and availability of location data will vary geographically and across service providers.

III. THE STATUTORY SCHEME

The Stored Communications Act (SCA) was enacted in 1986 as Title II of the Electronic Communications Privacy Act.[37] Although the SCA does not explicitly refer to historical CSLI,[38] historical CSLI is a "record or other information pertaining to a subscriber . . . or customer of [a provider of electronic communication service],"[39] and is subject to disclosure under 18 U.S.C. § 2703(c) and (d). As such, CSLI does not contain the content of any communication.[40] As originally enacted, the SCA provided for court ordered disclosure "only if the governmental entity show[ed] that there [was] reason to believe . . . the records or other information sought[] [were] *relevant* to a legitimate law enforcement inquiry."[41]

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) and amended the SCA to the current

34. Pell & Soghoian, *supra* note 18, at 128–29.

35. *Id.* at 128.

36. The law enforcement technique utilizes "triggerfish" technology. *See* William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 165–67 (2013).

37. *In re* United States for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 306 (3d Cir. 2010) [hereinafter *Sloviter Order*] (citing Stored Communications Act, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–11 (2006))).

38. *See* 18 U.S.C. §§ 2701–11.

39. *Sloviter Order*, 620 F.3d at 307–08.

40. 18 U.S.C. § 2703(c)(1).

41. Stored Communications Act, Pub. L. No. 99-508, § 207, 108 Stat. 1848, 1862 (1986) (codified at 18 U.S.C. § 2703(d)) (emphasis added).

intermediate standard.[42] The SCA now provides that a court may order disclosure of CSLI by the service provider if the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation."[43] The SCA also provides other mechanisms for disclosure of records and information pertaining to the subscriber, including pursuant to a warrant or the subscriber's consent.[44]

In addition to amending the SCA, CALEA amended § 3121 of Title 18 of the United States Code—the Pen Registers and Trap and Trace Devices Statute—and explicitly prohibited acquiring a subscriber's CSLI "solely pursuant to the authority for pen registers and trap and trace devices."[45] The Pen Registers and Trap and Trace Devices Statute authorizes the government to seek a court order for the installation of a pen register or a trap and trace device based on a certification that the "information likely to be obtained is relevant to an ongoing criminal investigation."[46] The terms "pen register" and "trap and trace device" are defined by the statute and include "dialing, routing, addressing, and signaling information."[47] In general terms, a pen register device records the numbers dialed—outgoing calls—and a trap and trace device records caller identifications—the numbers assigned to incoming calls.[48]

As noted above, *historical* CSLI can be disclosed under the SCA as a record or other information pertaining to the service provider's

---

42. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279, 4292 (1994) (codified as amended at 18 U.S.C. § 2703(d)); *see also Sloviter Order*, *supra* note 37, at 314 (noting that CALEA established intermediate standard).

43. 18 U.S.C. § 2703(d).

44. 18 U.S.C. § 2703(c)(1)(A)–(E).

45. Pen Registers and Trap and Trace Devices, 18 U.S.C. §§ 3121–3127 (2006); Communications Assistance for Law Enforcement Act § 103, 47 U.S.C. § 1002 (2006). The broader language provides that "with 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, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." *Id.*

46. 18 U.S.C. § 3122(b)(2).

47. 18 U.S.C. § 3127(3), (4).

48. H. MARSHALL JARRETT ET AL., U.S. DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 153, *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (last visited May 31, 2013).

subscriber or customer.[49] In order to obtain real-time information or information captured prospectively (after the date of a court order), however, the U.S. Department of Justice (DOJ) developed a "hybrid theory" drawing on the combined authority of the Pen Registers and Trap and Trace Devices Statute and orders issued under § 2703(d) of Title 18.[50] Because CSLI also meets the definition of "dialing, routing, addressing, or signaling information,"[51] the Pen Registers and Trap and Trace Devices Statute applies, but as noted above, it cannot be the sole authority for location information.[52] By combining the two statutes, the government could obtain a court order for prospective and real-time CSLI by applying both standards.[53] Pursuant to the Pen Registers and Trap and Trace Devices Statute, the government certifies that the information likely to be obtained is relevant to the investigation, and pursuant to § 2703(d), the government offers "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation."[54] As discussed in more detail below, the hybrid theory met with mixed results among federal magistrate and district court judges.[55]

In addition to the statutory authorities discussed above, CSLI may also be disclosed pursuant to a Rule 41 probable cause warrant or a wiretap order under Title III.[56] The relevant standards that the government must meet to acquire CSLI, therefore, range from: (1) demonstrating specific and articulable facts showing reasonable grounds that the information is relevant and material to the investigation (SCA);[57] (2) number one, plus a mere certification—rather than demonstration—that the information is likely to be relevant (SCA plus the Pen Registers and Trap and Trace Devices Statute);[58] (3) demonstrating probable cause to believe that the information will reveal "evidence of a crime," "contraband, fruits of [a] crime," or "property designed for use, intended for use, or used in committing a crime" (Rule 41);[59] or (4) number three plus other requirements such as demonstrating that other less intrusive

49. *See supra* text accompanying notes 37–41.
50. JARRETT ET AL., *supra* note 48, at 160.
51. *Id.*
52. *See supra* text accompanying note 45.
53. *See* JARRETT ET AL., *supra* note 48, at 160.
54. *Id.*
55. *See infra* text accompanying notes 65–70.
56. FED. R. CRIM. P. 41(d)(1); 18 U.S.C. § 2501 (2006).
57. 18 U.S.C. § 2703(d) (2006).
58. 18 U.S.C. § 3123(a)(1) (2006).
59. FED. R. CRIM. P. 41(c)(1)–(3).

investigative techniques have been tried and have failed, or why such methods reasonably appear unlike to succeed if tried, or would be too dangerous (Title III "super warrant").[60]

Although not directly relevant to obtaining CSLI, it is interesting to note that the Pen Registers and Trap and Trace Devices Statute allows the government to capture call information from within the private space of the home, which historically has revealed the location of the caller or the one receiving the call on a much lower standard—that is, the mere certification that the information is relevant to an ongoing criminal investigation.[61]

IV. JUDICIAL HODGEPODGE

The majority of the jurisprudence addressing the government's access to CSLI is provided by the hardworking United States Magistrate Judges across the country whose duties include issuing search warrants and other orders related to criminal investigations.[62] As of the end of 2012, only one reported circuit court case has dealt explicitly with the appropriateness of the SCA's intermediate standard for obtaining CSLI.[63] The breadth of conflict found in the existing case law highlights the need for congressional clarification.[64]

In early 2008, Magistrate Judge Lenihan summarized the then state of the case law on CSLI in a decision discussing both prospective and historical CSLI on behalf of all the magistrate judges in the Western District of Pennsylvania.[65] As Judge Lenihan pointed out, a

60. 18 U.S.C. § 2518(3)(c) (2006). "The federal wiretap statute, originally passed in 1968 and sometimes called 'Title III' or the Wiretap Act, requires the police to get a wiretap order—often called a 'super-warrant' because it is even harder to get than a regular search warrant—before they monitor or record your communications." ELECTRONIC FRONTIER FOUNDATION, *Wiretapping Law Protections*, SURVEILLANCE SELF-DEF., https://ssd.eff.org/wire/govt/wiretapping-protections (last visited May 31, 2013).

61. *See infra* text accompanying note 98.

62. As noted in Magistrate Judge Smith's testimony, there are over 500 magistrate judges in the federal district courts whose duties include hearing civil matters and almost all criminal matters except conducting felony trials. *ECPA Hearing*, *supra* note 1, at 79 (statement of United States Mag. J. Smith).

63. *See Sloviter Order*, *supra* note 37, at 314.

64. Because this issue has generated voluminous case law, the author does not attempt to provide an analysis including all available cases, but rather has endeavored to focus on cases that will enhance further discussion about (at least some of) the critical issues. *See* cases cited *infra* note 67.

65. *See In re* The United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 543 F. Supp. 2d 585, 599–600 (W.D. Pa. 2008) [hereinafter *Lenihan Order*]. As discussed more fully below, the Court of Appeals for

"significant majority" of the courts had denied the government access to prospective and real-time location information based on the hybrid theory, which, as noted above, combines the authority under the Pen Registers and Trap and Trace Devices Statute and the SCA.[66] Even magistrate judges within the same district disagreed over the applicable standard for obtaining prospective CSLI.[67] With regard to historical CSLI, decisions granting the government access had, for the most part, concluded without analysis or merely suggested that the government could obtain CSLI under the SCA.[68] Judge Lenihan distinguished the reported opinions of two district court judges that had specifically addressed and allowed the government to obtain historical CSLI under the SCA.[69] Judge Lenihan held, in part, that because the cell phone was a "tracking device" under 18 U.S.C. § 3117, the communications from which are expressly excluded from the SCA, the government could only obtain the CSLI, *whether*

---

the Third Circuit vacated Judge Lenihan's order in *Sloviter Order*, *supra* note 37. In discussing Judge Lenihan's opinion, the court began by noting that the fact that the opinion was joined by the other district court magistrate judges was "unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues . . . ." *Id.* at 308.

66. *See Lenihan Order*, *supra* note 65, at 599; *supra* notes 40–41.

67. *Compare In re* The United States for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 488 (S.D.N.Y. 2005) (accepting hybrid theory), *with In re* The United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006) (rejecting hybrid theory and noting that "prospective cell site location information has been the subject of at least ten prior decisions by Magistrate Judges in this Circuit and around the country"). Ultimately, the disagreement in the Southern District of New York was resolved in favor of the hybrid theory by Judge Kaplan in *In re The United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 463 (S.D.N.Y. 2006). However, Judge McMahon expressly disagreed with Judge Kaplan in *In re The United States for an Order Authorizing Use of a Pen Register with, Caller Identification Device Cell Site Location Auth. on a Cellular Tel.*, 2009 WL 159187, at *5 (S.D.N.Y. Jan. 13, 2009), finding that CSLI did not constitute a record and that it was a tracking device.

68. *See Lenihan Order*, *supra* note 65, at 600; *see also ECPA Hearing*, *supra* note 1 (statement of United States Mag. J. Smith).

69. *Lenihan Order*, *supra* note 65, at 604–05 n.53 (citing *In re* The United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007) [hereinafter *Stearns Order*]; *In re* The United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411 (S.D. Tex. 2007) [hereinafter *Rosenthal Order*]).

prospective or historical, with a warrant pursuant to a showing of probable cause.[70]

Prior to Judge Lenihan's opinion, Judge Stearns from the District of Massachusetts and Judge Rosenthal from the Southern District of Texas had overturned magistrate judges' decisions refusing access to CSLI without a probable cause warrant.[71] Both specifically addressed the required standard and upheld the government's access to CSLI based on the government's proffer of specific and articulable facts demonstrating reasonable grounds that the information was relevant and material to an ongoing criminal investigation under the SCA.[72] Judge Stearns, in allowing the disclosure of historical CSLI, first determined that the SCA applies to historical CSLI.[73] The judge then went on to determine that a demonstration of probable cause under the Fourth Amendment was not required because the government sought only historical information about the subject's location in the past.[74] Further, the court noted that even if the government sought prospective information that allowed the government to "track" the cell phone into a protected area such as the home, "there is nothing presumptively illegal about the possession of a cellular phone," and "[t]he most that the 'tracked' cell phone might reveal is that its owner might presently be found in the home."[75] The court went on to conclude that "[t]here is nothing, however, about that disclosure that is any more incriminating or revealing than what could be gleaned from the activation of a pen register or from physical surveillance. Moreover, outside of the home it is doubtful that the tracking of a cell phone has any Fourth Amendment implication whatsoever."[76]

Following Judge Stearns' decision, Judge Rosenthal—noting the division among magistrate judges and district court judges and the need for additional guidance to the courts and prosecutors—issued an opinion, which discussed access to both prospective and historical CSLI.[77] Judge Rosenthal began by finding that the government had met its statutory burdens under both the Pen Registers and Trap and

70. *Id.* at 589, 594–95, 601–607.
71. *Stearns Order*, *supra* note 69, at 81–82; *Rosenthal Order*, *supra* note 69, at 412, 418.
72. *See Stearns Order*, *supra* note 69, at 81–82 (allowing disclosure of historical CSLI); *Rosenthal Order*, *supra* note 69, at 418 (allowing disclosure of both historical and prospective CSLI, based on limited information sought by the government).
73. *Stearns Order*, *supra* note 69, at 79–80.
74. *Id.* at 81.
75. *Id.*
76. *Id.*
77. *Rosenthal Order*, *supra* note 69, at 412–13.

Trace Devices Statute as well as the SCA by certifying that the information likely to be obtained was relevant to an ongoing criminal investigation and by providing specific and articulable facts showing reasonable grounds that the information sought was relevant and material to the investigation, respectively.[78] The judge then went on to address whether the government had to demonstrate the higher standard of probable cause.[79]

Judge Rosenthal acknowledged other courts' concerns that CSLI might be used to turn the cell phone into a tracking device.[80] He noted, however, that the cases granting applications for CSLI did so on a limited basis to "minimiz[e] the concern that a cell phone could be used as a kind of 'tracking device.'"[81] Just as in prior cases from the Southern District of New York and the Western District of Louisiana, which were based on similar facts and resulted in the grant of the government's request,[82] in the case before Judge Rosenthal, the government did not seek information from multiple towers (thus allowing triangulation), GPS activation, or other information that would allow continuous tracking when the cell phone was not placing a call.[83] The court further required that the information could only be provided to the government after the cellular service provider recorded and stored the information.[84]

In response to Magistrate Judge Lenihan's 2008 decision and following an appeal in which the district court affirmed the decision without analysis, the Court of Appeals for the Third Circuit issued the first appellate decision to address whether a court can deny the government's access to historical CSLI once the government has met its burden under the SCA.[85] In sum, the court rejected Judge

78. *Id.* at 414–18.

79. *Id.* at 414.

80. *Id.* at 415.

81. *Id.* at 415–16 (quoting *In re* The United States for an Order (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006) [hereinafter *Rosenthal I Order*]).

82. *Id.* at 416.

83. *Id.* at 417–18.

84. *Id.* at 419.

85. *Sloviter Order*, *supra* note 37, at 305–06. Prior to the Third Circuit opinion, the Court of Appeals for the Sixth Circuit rejected suppression of cell site location information obtained when an agent dialed the suspect's cell number after losing visual contact with him. *See* United States v. Forest, 355 F.3d 942 (6th Cir. 2004). However, the case did not involve access to CSLI under the SCA, but rather challenges under Title III, 18 U.S.C. § 3117, and the Fourth Amendment. *Id.* at 949. Most notably, the court found that

Lenihan's reasoning and her interpretation of the legislative history and held that the government was not required to demonstrate probable cause and could obtain historical CSLI based on the SCA's intermediate standard.[86] In reaching its decision, the court noted that even if historical CSLI allowed an inference of the present or future location of a person, and thus resembled a tracking device, the "privacy interests at issue [in Fourth Amendment precedents] are confined to the interior of the home" and such privacy issues were not present in the record before the court.[87] The court, therefore, rejected Judge Lenihan's conclusion "that CSLI by definition, should be considered information from a tracking device that, for that reason, requires probable cause for its production."[88]

Although the Third Circuit affirmed the government's access to historical CSLI under the SCA,[89] the court did not stop there. The court rejected the government's argument that the court is *required* to issue an order for CSLI if the government meets its burden of providing specific and articulable facts showing reasonable grounds to believe that the information sought is relevant and material to the ongoing criminal investigation.[90] First, the court looked to the language of 18 U.S.C. § 2703(d) that states "a 'court order for disclosure . . . *may be* issued by any court . . . of competent jurisdiction and *shall* issue *only if*' the [above] intermediate standard is met."[91] The court found that this is a permissive standard that sets a necessary but not automatically sufficient condition.[92] Further, since § 2703(c)(1)(A) provides the option for disclosure of the information pursuant to a warrant, the court was "unwilling to remove that option" and held that magistrate judges have the discretion to require a warrant showing probable cause.[93]

> [T]he distinction between the cell-site data and Garner's location is not legally significant under the particular facts of this case. Here, the cell-site data is simply a proxy for Garner's visually observable location. But as previously noted, Garner had no legitimate expectation of privacy in his movements along public highways.

Id. at 951. Similarly, in *United States v. Skinner*, the Sixth Circuit rejected a Fourth Amendment challenge to CSLI obtained through a court order. United States v. Skinner, 690 F.3d. 772, 775 (6th Cir. 2012).

86. *Sloviter Order*, *supra* note 37, at 314–15.
87. *Id.* at 312–13.
88. *Id.* at 313.
89. *Id.* at 312–13.
90. *Id.* at 315.
91. *Id.*
92. *Id.*
93. *Id.* at 319.

Nevertheless, the court directed that a warrant "is an option to be used sparingly because Congress also included the option of a § 2703(d) order."[94]

In rejecting the government's claim that the warrant option only referred to the prosecutor's discretion to issue one form of process, the court noted:

> The Government's position would preclude magistrate judges from inquiring into the types of information that would actually be disclosed by a cell provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home.[95]

Although concurring in the result and most of the reasoning, Judge Tashima wrote a concurring opinion that highlights some important points.[96] Judge Tashima was concerned that the majority's opinion provided "*no* standards for the approval or disapproval of an application for an order under § 2703(d) . . . [and] vest[ed] magistrate judges with . . . uncabined discretion to grant or deny" the issuance of the order.[97] Further, Judge Tashima was of the view

> that the magistrate may refuse to issue the § 2703(d) order here only if she finds that the government failed to present specific and articulable facts sufficient to meet the standard . . . or, alternatively, finds that the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of his home.[98]

Additionally, Judge Tashima noted that the magistrate should be permitted to issue a conditional order requiring minimization of such information.[99]

A few months before the Third Circuit issued its opinion in the *Sloviter* decision, Magistrate Judge Austin in the Western District of Texas joined the growing list of magistrate judges to produce a

94. *Id.*
95. *Id.* at 317.
96. *Id.* at 319–21 (Tashima, J., concurring).
97. *Id.* at 320.
98. *Id.*
99. *Id.* at 320 n.10.

lengthy opinion highlighting some of the legal issues permeating requests for orders under 18 U.S.C. § 2703(d).[100] In addition to providing a summary of the case law to date,[101] Judge Austin found that a cell phone is a "tracking device" under 18 U.S.C. § 3117(b) and held that the government's requests for CSLI, *whether prospective or historical*, would only be granted pursuant to a warrant based on probable cause as required by Rule 41.[102] Judge Austin acknowledged that other courts had issued orders for CSLI using the SCA's intermediate standard by distinguishing between CSLI from a single cell tower and CSLI from multiple towers allowing for triangulation (and greater precision) or GPS data.[103] The judge concluded, however, that, due to advancing technology, these distinctions were "academic."[104]

In reaching this conclusion, Judge Austin highlighted an important—but rarely discussed—legal question: What does "probable cause" mean in the context of a warrant for CSLI? [105] Judge Austin noted that in many warrant applications for CSLI, the typical statement of probable cause set forth in the affidavit provides:

> (1) there is evidence that the user of the target phone is dealing in narcotics; (2) there is evidence that the target phone is used in the narcotics dealing; and (3) being able to track the user's movements would assist in the investigation (for example, by helping to identify associates, stash houses, or sources of supply).[106]

The judge further explained, "On its face, this may seem adequate to support the issuance of a warrant for CSLI. On closer inspection, however, this conclusion is not so clear."[107] Judge Austin then discussed the opinion of Magistrate Judge Facciola of the United States District Court for the District of Columbia, in which the judge declined to issue a warrant because the information sought was not

100. *See In re* The United States for an Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; (3) Authorizing Disclosure of Location Based Services, 727 F. Supp. 2d 571, 572 (W.D. Tex. 2010) [hereinafter *Austin Order*].

101. *See Id.* at 573–75.

102. *Id.* at 578–79, 583–84 & n.21.

103. *Id.* at 574.

104. *Id.* at 580.

105. *Id.* at 581.

106. *Id.*

107. *Id.*

"*evidence of a crime*" but rather evidence that would be relevant and admissible in the criminal case.[108] Judge Austin then analyzed the parts of Rule 41 dealing with search and seizure of persons or property and warrants for tracking devices, as well as the case law on tracking devices.[109] Noting that "there are difficult questions presented by the probable cause determination on CSLI applications," to which the answers are not obvious, the judge fashioned a "cautious approach" pending "more guidance from Congress and the courts on [the] issues."[110] Ultimately, Judge Austin held that a warrant for CSLI could be based on a showing of "probable cause to believe that tracking the phone will *lead* to evidence of a crime."[111] Nevertheless, more is needed than evidence simply demonstrating that "a person has a cell phone and is engaged in criminal conduct."[112]

The meaning of "probable cause" was raised again in a case before Magistrate Judge Gauvey in the District of Maryland.[113] In that case, the government sought prospective precise location information pursuant to the Fourth Amendment and Rule 41, the SCA, and the All Writs Act (pertaining to the inherent authority of the court) in order to execute an arrest warrant.[114] The government advanced two arguments for obtaining the information under the Fourth Amendment: first, that it was entitled to the information pursuant to the arrest warrant, and second, that it could seek a search warrant to obtain evidence in furtherance of apprehending the defendant.[115]

The court held that the arrest warrant alone did not authorize the government to obtain the location information, and a search warrant was not authorized since the government did not seek any information that was evidence of a crime.[116] Had the government provided evidence that the defendant was a fugitive and was fleeing to avoid prosecution in violation of 18 U.S.C. § 1073, in which case the defendant's location would have been evidence of his crime of flight, a search warrant would have authorized.[117] In addition, although a search warrant could have been issued based on probable

108. *Id.* at 581–82; *see also In re* The United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006).
109. *Austin Order*, *supra* note 100, at 582–83.
110. *Id.* at 583.
111. *Id.* at 584.
112. *Id.*
113. *Gauvey Order*, *supra* note 8, at 530.
114. *Id.*
115. *Id.* at 535–36.
116. *Id.* at 536.
117. *Id.* at 537.

cause that the defendant was at a specific location,[118] that was the very issue the government wished to resolve.

In discussing a warrant for location information, the court noted a "vehement" disagreement between the parties about the nature of the requisite probable cause.[119] The government asserted that probable cause that the evidence sought would aid in the apprehension of the defendant was sufficient.[120] The Federal Public Defender's Office took the position that the government must establish a reasonable probability that the information sought constitutes proof of a crime, that is, that there must be a nexus between the item seized and the criminal behavior.[121] The court ultimately concurred with the defense.[122]

The court recognized the government's "laudable societal goal of bringing a charged defendant to justice," but the court deemed it "an exercise of police power neither clearly envisioned in the Fourth Amendment nor approved by the courts, in an area of quickly shifting, complex technology."[123] In its discussion, the court noted that Professor Orin Kerr, in hearings in 2010 before the House Committee on the Judiciary on Electronic Communications Privacy Act reform, had raised the exact issue of the meaning of probable cause.[124] Professor Kerr had asked:

> . . . *[P]robable cause of what?* Is that probable cause to believe the person tracked is guilty of a crime? Or is it probable cause to believe the evidence of location information obtained would *itself* be evidence of a crime? The difference is important. *In the case of a search warrant, "probable cause" generally refers to probable cause to believe that the information to be obtained is itself evidence of a crime.* But cell phone location information will itself be evidence of crime only in specific kinds of cases. For example, *such information normally will not be evidence of a crime if investigators want to obtain the present location of someone who committed a past crime.*

118. *Id.* at 550.
119. *Id.* at 560.
120. *Id.*
121. *Id.* at 560–61.
122. *Id.* at 561.
123. *Id.* at 564.
124. *Id.* at 560 (internal citations omitted).

> To see this, imagine the police have probable cause to arrest a criminal for a crime committed last week. The police want to locate the suspect in order to arrest him. In that case, the police will not have probable cause to believe that the location of the criminal's cell phone is itself evidence of a crime. The suspect's location a week after the crime occurred does not give the police any information indicating that the suspect did or did not commit the crime. But if the police have probable cause to arrest someone, and they know his cell-phone number, I would think the law should allow the government some way of locating the suspect pursuant to an appropriate court order. A requirement that location information be obtainable only based on probable cause to believe that the location information is itself evidence of a crime would not seem to allow that.[125]

The court further noted that although Professor Kerr had identified the issue, he did not offer any solution, nor did any lawmakers in proposed legislation that followed.[126] With respect to the SCA, the court joined other jurisdictions holding that where prospective, real-time location information is sought, the cell phone is a tracking device and subject to the requirements of Rule 41 and the Fourth Amendment.[127]

The decision in *United States v. Maynard*,[128] and subsequent Supreme Court decision in *United States v. Jones*,[129] resulted in courts revisiting the standards for access to historical CSLI. Magistrate Judge Orenstein, in the Eastern District of New York, was one of the first to question the appropriate standards for historical CSLI in light of the *Maynard* case.[130] Judge Orenstein had previously granted applications for historical CSLI under the intermediate SCA standard while requiring the government to establish probable cause in an application for prospective CSLI.[131] The *Maynard* decision disturbed the uniformity among the circuits—which did not require a warrant for tracking outside of the home—when it held that GPS

125. *Id.* (quoting *ECPA Hearing*, *supra* note 1, at 39–40 (statement of Orin Kerr, Professor, George Washington University Law School)).

126. *Id.* at 564.

127. *Id.* at 577.

128. United States v. Maynard, 615 F.3d 554, 549 (D.C. Cir. 2010), *aff'd in part sub. nom.* United States v. Jones, 132 S. Ct. 945 (2012).

129. United States v. Jones, 132 S. Ct. 945, 949 (2012).

130. *In re* The United States for an Order Authorizing Release of Historical Cell-site Info., 736 F. Supp. 2d 578 (E.D.N.Y. 2010) [hereinafter *Orenstein Order*].

131. *Id.* at 580.

tracking information was obtained in violation of the Fourth Amendment; thus, the judge was compelled to re-analyze the issue.[132]

Judge Orenstein reaffirmed his prior conclusion that "*as a statutory matter* the SCA permits a court to issue the order [for historical CSLI] without a showing of probable cause," but found the *Maynard* reasoning persuasive and the government's efforts to distinguish it from the instant case unavailing.[133] Accordingly, the judge held that the Fourth Amendment required a warrant based on probable cause.[134]

Next, Magistrate Judge Stephen William Smith in the Southern District of Texas[135] followed Judge Orenstein's suggestion that "courts re-examine the constitutionality of historical cell site requests in light of recent appellate court decisions," including *Maynard*.[136] In determining consolidated requests for historical CSLI under the SCA in three criminal investigations, Judge Smith held that, although he had previously granted such requests, the "earlier interpretation of the SCA is now constitutionally impermissible."[137] Judge Smith began by documenting the vast developments in location technology in his "Findings of Fact."[138] Since prior decisions allowing historical CSLI without a warrant relied on imprecise location data, Judge Smith observed that "the continuing vitality of those decisions must be doubted." [139]

The judge ultimately concluded that CSLI was "squarely within the protective ambit of *United States v. Karo*," because the CSLI would reveal information about constitutionally protected spaces.[140] Although finding that reliance on the *Maynard* case was not "essential," Judge Smith proceeded to analyze the case and concurred in Judge Orenstein's "holding that *Maynard*'s prolonged surveillance doctrine precludes the Government from obtaining two months of cell phone tracking data without a warrant."[141] Judge Smith, thus, based his decision that warrantless disclosure of CSLI violates the

132. *Id.* at 581–82.
133. *Id.* at 584–95.
134. *Id.* at 579.
135. *See, e.g., In re* The United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010).
136. *Id.* at 830, 840.
137. *Id.* at 829 & n.2.
138. *Id.* at 831–35.
139. *Id.* at 837.
140. *Id.* at 836–38.
141. *Id.* at 838, 840.

Fourth Amendment on two independent grounds: *Karo* and *Maynard*.[142]

As noted by my colleague in *Post*-Jones: *How District Courts Are Answering the Myriad Questions Raised by the Supreme Court's Decision in* United States v. Jones, the decision left many questions unanswered.[143] The majority's decision, reverting to a trespass theory on physical property, does little to elucidate the implications of using CSLI in criminal investigations. Perhaps the best that might be gleaned is that the Court may revisit the third-party doctrine, which holds that a person loses her reasonable expectation of privacy in information voluntarily revealed to third parties.[144]

Since *Jones*, courts analyzing access to historical CSLI have been reluctant to extend Fourth Amendment protections to such information. The court in *United States v. Graham* rejected the defendant's claim that his Fourth Amendment rights were violated when the government obtained historical CSLI without a warrant based on probable cause.[145] The court noted that prior decisions were divided among: (1) those which found that the Fourth Amendment was implicated and a showing of probable cause was required under *certain circumstances*, particularly if the information covered a sufficiently long period of time, thus implicating a person's reasonable expectation of privacy; and (2) decisions finding the SCA's intermediate standard sufficient regardless of the time period involved because the information constituted a business record held by third parties and voluntarily conveyed by the person.[146] The court highlighted two important distinctions between *Maynard* and the instant case.[147] First, *Maynard* involved real-time monitoring of the suspect's location as opposed to historical location information,[148]

142. *Id.* at 846. Judge Smith also rejected the government's argument that the Fourth Amendment was not implicated because the records were voluntarily conveyed to the provider. *Id.* at 840–45.

143. Jason D. Medinger, *Post-Jones: How District Courts are Answering the Myriad of Questions Raised by the Supreme Court's Decision in* United States v. Jones, 42 U. BALT. L. REV. 395 (2013).

144. *Compare* United States v. Jones, 132 S. Ct. 945, 951–52 (2012), *and* United States v. Knotts, 460 U.S. 276, 280–84, (1983), *with Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

145. United States v. Graham, 846 F. Supp. 2d 384, 385, 387, 389, 396–97, 406 (D. Md. 2012).

146. *Id.* at 388–89 (emphasis added).

147. *Id.* at 391–92.

148. *Id.*

and second, the SCA incorporates judicial review, which was not present in *Maynard*.[149]

In discussing the *Jones* case, the court concluded that although a five justice majority appeared "willing to accept the principle that government surveillance over time *can* implicate an individual's reasonable expectation of privacy . . . the factual differences [between the technologies] lead this [c]ourt to proceed with caution in extrapolating too far from the Supreme Court's varied opinions in *Jones*."[150] Because access to "historical [CSLI] did not involve a physical trespass," the court then proceeded to "analyze the Fourth Amendment implications of the [SCA] under the *Katz* test," as directed by the *Jones* case.[151]

After a thorough discussion of the Supreme Court and Fourth Circuit precedents, as well as the mosaic theory, the court concluded that the third-party doctrine applied to historical CSLI and that, as business records kept in the ordinary course of business, no legitimate expectation of privacy in the records existed and no Fourth Amendment violation occurred.[152] In addition, the court analyzed and rejected the approach of Judge Garufis in the Eastern District of New York, who, in the wake of *Maynard,* found an exception to the third-party doctrine and held that the government was required to obtain a search warrant based on probable cause for historical CSLI.[153] Most notably, Judge Bennett, while acknowledging Judge Alito's statement in *Jones* that "'the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,'" went on to state:

> [T]he law as it now stands simply does not contemplate a situation whereby traditional surveillance becomes a Fourth

149. *Id.* at 392.

150. *Id.* at 394.

151. *Id.* at 396.

152. *Id.* at 400, 403; *see also* United States v. Ruby, No. 12CR1073(WQH), 2013 WL 544888, at *6 (S.D. Cal. Feb. 12, 2013) (holding that the defendant had no reasonable expectation of privacy in cell site information, which was voluntarily conveyed to a third party business); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8–9 (S.D. Fla. July 30, 2012) (holding that the defendant had no legitimate expectation of privacy in cell phone data that he voluntarily turned over to a third party).

153. *Graham*, 846 F. Supp. 2d at 401; *see also In re* The United States for an Order Authorizing the Release of Historical Cell-site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) (concluding that defendants have a sufficiently protected privacy interest in CSLI to warrant an exception to the third party doctrine).

> Amendment "search" only after some specified period of time—discrete acts of law enforcement are either constitutional or they are not. . . . The fact of the matter is that in enacting the Stored Communications Act, Congress passed a law that rejects a warrant requirement for this type of information, but does require specific and articulable facts to be determined by a judicial officer.
>
> Further, it is entirely unclear what the implications would be of an interpretation of the Fourth Amendment that protects "cumulative" data collected by law enforcement. Taken to its logical extreme, such a reading would theoretically affect entire police investigations, and not just surveillance via cell site location data. In *Jones,* Justice Alito stated that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," but goes on to conclude that "the line was surely crossed" when that monitoring continued for four weeks. *If that is how the Fourth Amendment is to be interpreted, then the police could commit a constitutional violation by taking enough individually permissible steps, that in the aggregate, add up to a substantial amount of data being collected on a suspect—thereby infringing his reasonable expectation of privacy.* For example, using only ordinary investigatory techniques, police can (and do) collect vast amounts of data on criminal suspects. After interviewing witnesses, conducting surveillance (perhaps enhanced by discrete requests for historical cell site location records under the Stored Communications Act), and reviewing pen registers and bank records, police may be able to paint an "intimate picture" of a person's life. Under the mosaic theory, at some point this collection of data would *become* a Fourth Amendment search at some undefined point.[154]

More succinctly, as pointed out by Professor Kerr, "[T]he mosaic theory has the bizarre consequence of creating retroactive unconstitutionality."[155]

Finally, two other points made by the court are worth mentioning. First, the court noted that "even if cell site records could definitively

154. *Graham*, 846 F. Supp. 2d at 401(first emphasis added) (citations omitted).

155. *Id.* at 402.

indicate that an individual is in his home, that information only reveals that a person made or received a phone call while at home—in other words, non-incriminatory information that is clearly obtainable via the . . . pen register."[156] Second, the court highlighted the importance of legislative—not judicial—solutions to privacy concerns stemming from rapidly developing technologies.[157]

Since *Jones*, other courts have come to the same conclusion that historical CSLI records are afforded no Fourth Amendment protection.[158] Magistrate Judge Collings, in the District of Massachusetts, recently revisited the issue in light of *Jones*.[159] Noting that probable cause had not been required for such records since Judge Stearns' decision in 2007, Judge Collings nevertheless wrote to highlight the difficult question of what constitutes a reasonable expectation of privacy in our electronic age and the eventual and inevitable resolution by either the Supreme Court or Congress.[160] Judge Collings concluded that the best approach was counseled by Judge Bennett in *Graham,* who had relied on the Supreme Court's caution that the judiciary should not prematurely elaborate on Fourth Amendment implications in the wake of emerging technology.[161] Thus, Judge Collings reiterated that Judge Stearns' opinion would be followed "[u]ntil either the First Circuit Court of Appeals or the Supreme Court rule[s] otherwise, or Congress enacts legislation dealing with the problem."[162]

As noted previously, after the *Maynard* decision, Magistrate Judge Smith[163] revisited the constitutionality of applications for historical CSLI and concluded that warrantless disclosure of CSLI violates the Fourth Amendment. The district court subsequently adopted Judge

156. *Id.* at 404.

157. *Id.* at 404–05 ("When technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes. . . . [T]he legislative branch rather than the judiciary should create the primary investigative rules when technology is changing.") (quoting Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004)).

158. *See, e.g.*, United States v. Ruby, No. 12CR1073(WQH), 2013 WL 544888, at *6 (S.D. Cal. Feb. 12, 2013); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012).

159. *In re* The United States for an Order Pursuant to Title 18, United States Code, Section 2703(D) to Disclose Subscriber Info. & Cell Site Info., 849 F. Supp. 2d 177 (D. Mass. 2012).

160. *Id.* at 178.

161. *Id.* at 179.

162. *Id.*

163. *See supra* text and accompanying notes 119-120.

Smith's ruling that § 2703(d) orders for CSLI are unconstitutional and the government appealed to the Fifth Circuit.[164] The Fifth Circuit issued its opinion on July 30, 2013, while this article was pending publication.[165]

The Fifth Circuit began by disagreeing with the Third Circuit's conclusion that the court has discretion to deny the government's request for a court order based on the lesser SCA standard and require a warrant based on probable cause.[166] As to the constitutional question, the court found that CSLI constitutes business records of voluntarily conveyed information and therefore is not protected by the Fourth Amendment.[167]

Finally, the court acknowledged that technological advances can impact reasonable expectations of privacy but expressly declined to create its own rule contrary to the legislative solution enacted in the SCA.[168] The court instead decided the case on the narrow grounds before it holding that "Section 2703(d) orders to obtain *historical* [CSLI] for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional."[169]

V. FINDING THE BALANCE

"When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[170] It is hard to argue with the fundamental principle in Judge Rogers' statement. In *United States v. Skinner*, Judge Rogers held that there was simply no reasonable expectation of privacy in the CSLI at issue in the case.[171] The district court had affirmed Magistrate Judge Guyton's opinion and concurred in his analysis of the issues.[172] The district court held, "[A]ssuming that a search occurred when the government utilized cell-site data to locate and track defendant's vehicle as it traveled

164. *In re* The United States for historical cell site data, 724 F.3d 600, 605 (5th Cir. 2013).
165. *In re* The United States for historical cell site data, 724 F.3d 600 (5th Cir. 2013).
166. *Id.* at 604–05.
167. *Id.* at 606–09.
168. *Id.* at 609.
169. *Id.*
170. United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).
171. *Id.*
172. United States v. Skinner, No. 3:06-CR-100, 2007 WL 1556596 at *1 (E.D. Tenn. May 24, 2007).

upon public highways, the defendant lacked standing to assert a Fourth Amendment protected interest in the cell phone data . . . ."[173]

The case, involving an extensive marijuana drug trafficking organization, is a model for the criminal use of cell phones. The source of the marijuana bought pay-as-you-go cell phones with false names and addresses, programmed them with the criminal cohorts' contact information, and distributed them to the couriers and other participants.[174] They routinely discarded them and obtained new ones with different numbers in different names.[175] The source did not know that the phones were equipped with GPS technology.[176] The ultimate demise of the organization occurred when one of the phones was identified in a wiretap interception as used by a courier soon to be en route with a load of marijuana.[177] Drug Enforcement Administration agents obtained a court order under 18 U.S.C. § 2703(d) and tracked the phone as it traveled across the country with drugs, ultimately intercepting it in Texas en route to Tennessee.[178]

No one can question that extensively detailed—geographical and temporal—real-time, or historical location information in the hands of law enforcement, or non-governmental entities for that matter, raises legitimate privacy concerns. At the same time, the courts and Congress alike have frequently recognized that law enforcement investigative interests and needs in furtherance of protecting the public should not be unduly hindered but rather carefully balanced with the privacy interests of the public it serves.[179] There is also little question that rapid technological developments over the last two decades provide increasingly sophisticated tools that can further both criminality and law enforcement efforts seeking to interdict that criminality in the interest of public safety and the reduction of violent crime.

The federal magistrate judges reviewing requests for orders for CSLI have grappled with these issues in an ever changing landscape of highly technical information and in the wake of *Maynard*'s

173. *Id.*
174. *Skinner*, 690 F.3d at 775.
175. *Id.*
176. *Id.*
177. *Id.* at 776.
178. *Id.*
179. *See, e.g.*, *Lenihan Order*, *supra* note 65, at 587; *ECPA Hearing*, supra note 1, at 4–5; S. REP. 99-541, at 5 (1986).

recognition that real-time, highly accurate monitoring over an extended time period potentially reveals sensitive details about a person's life. The courts' efforts have been further exacerbated by the very nature of CSLI data, which can lead to uncertainty and confusion about the precision of the location information sought by the government as an initial matter and the specific information ultimately available for production by the cellular service provider.[180] The resulting jurisprudence, while frequently thorough and thoughtful, is largely unsettled. Courts have become increasingly wary, and rightfully so, about Fourth Amendment implications arising from intensive real-time or historical monitoring over extended periods of time. Yet the courts are cautious about straying too far from the guidance in *Jones* in addressing Fourth Amendment concerns arising from emerging technology.[181]

The role of the courts in granting law enforcement access to potentially intrusive techniques will forever remain a fact-driven analysis in which the courts must engage. The variable nature of CSLI and its rapidly developing technology add additional elements to the shifting fact-based analysis the courts will continue to be saddled with in evaluating government requests for CSLI. Nevertheless, the courts and law enforcement would significantly benefit from legislative clarification of static issues, such as whether a cell phone can ever be a tracking device within the meaning of 18 U.S.C. § 3117. Moreover, legislation could address whether prospective and real-time CSLI are obtainable under a § 2703(d) order, as well as the government's burden in acquiring such CSLI.

Whether prospective or historical CSLI is at issue, courts and Congress should be cautious in requiring a warrant based on probable cause without a thorough analysis of the issues and ramifications. In oral argument before the United States Court of Appeals for the Fifth Circuit in *In Re: Application of the United States for Historical Cell Site Data*, the court asked the government why it could not simply

180. *See supra* text and accompanying notes 20–24 (discussing how the cell site density impacts the precision of data); *e.g.*, *Owsley Order*, *supra* note 33, at *1, 4 (criticizing government for not understanding the technology in CSLI applications); *In Re* The United States for Historical Cell Site Data, No. 11-20884, Oral Arguments (Oct. 2, 2012), *available at* http://www.ca5.uscourts.gov/OralArgumentRecordings.aspx (judge questions what CSLI information is actually requested pursuant to § 2703(d) application for order).

181. *See supra* notes 141–145 (discussing *Graham* and other post-*Jones* decisions).

seek a warrant.[182] Counsel for the government noted that a warrant would require probable cause that the search would reveal evidence of a crime whereas the CSLI order would only require the government to provide specific and articulable facts that the information would be relevant and material to the investigation.[183] The government then offered the hypothetical example of a kidnapping where the parents had suspicions or concerns about a particular individual.[184] Assuming the parents could point to some specific facts underpinning the concerns, the government could meet the latter standard but not the former.[185] Another example discussed by the government involved a case in which, although the CSLI was only accurate to within a few blocks, the CSLI confirmed that the suspect traveled to another town to steal cars for use in the crime.[186]

Yet another frequent example arises during the early stages of an investigation when law enforcement agents have viable leads about an individual's illegal activity but have very little information with which to identify the suspect, perhaps merely a nickname, cell phone number, and general area of operation. CSLI could confirm the suspect's identity and lead to other relevant evidence or exonerate the suspect.

These examples involve historical, prospective, and real-time CSLI, without which the investigations could be significantly hindered. In the kidnapping example, the use of CSLI could make the difference between the successful recovery of the victim unharmed and otherwise. There are no doubt other examples in which the warrant standard cannot be met and its application will unduly hinder law enforcement.

Even if Congress or the courts conclude that the higher warrant/probable cause standard should be imposed on the government's requests for CSLI, access to CSLI will be available only in limited circumstances absent a clarification of "probable cause" in this context. As noted above, Magistrate Judge Austin confronted this problem and ultimately held that the warrant for CSLI

182. *In re* United States for Historical Cell Site Data, No. 11-20884, Oral Arguments (Oct. 2, 2012), *available at* http://www.ca5.uscourts.gov/OralArgumentRecordings.aspx (recordings of oral arguments at approximately at 44 minutes).

183. *Id.*

184. *Id.*

185. *Id.*

186. *Id.*

would be issued based on probable cause that the information would *lead* to evidence of a crime.[187] Modification of the warrant/probable cause standard in an era of rapid technological change could lead to a watering down of the standard.

Many of the issues raised by law enforcement's use of precise CSLI are not subject to a simple fix. Whether applying a warrant/probable cause standard or the lesser § 2703(d) standard, judicial oversight is required for the release of CSLI. This provides the requisite neutral determination to protect Fourth Amendment rights. As noted above, the Third Circuit held that a court may approve the request on the lesser standard or ask the government to meet a probable cause standard.[188] This may be the wisest approach and would allow further development of the law in this complex area. Given the fact-intensive nature of either determination, federal magistrate judges will always be engaged in this process. It is incumbent upon the government to come to the court with the best information it can obtain about the CSLI available from the service providers and to limit its requests to time periods reasonable to accomplish its investigative goals. Further, the government needs to assuage the court's concerns by providing proactive minimization procedures to acknowledge and address potential capturing of CSLI in protected areas that are irrelevant to the investigation or of individuals that are unrelated to the investigation.[189] By proactively applying prophylactic measures and requesting reasonable temporal data, the government and courts can work together—at least in the short term—to strike the balance between reasonable government access to critical investigative information and legitimate privacy concerns.

187. *See supra* text accompany note 106.

188. *See supra* text accompanying notes 85–94. In addition, a consolidated appeal of several of Magistrate Smith's denials of applications for 2703(d) orders is pending before the United States Court of Appeals for the Fifth Circuit in Case No. 11-20884.

189. *See Owsley Order*, *supra* note 33, at *4 (criticizing the government for not articulating a plan for the data captured related to innocent persons).