Michigan Telecommunications and Technology Law Review

Volume 21 | Issue 2

2015

No More Shortcuts: Protect Cell Site Location Data with a Warrant Requirement

Lauren E. Babst
University of Michigan Law School

NOTE

NO MORE SHORTCUTS: PROTECT CELL SITE LOCATION DATA WITH A WARRANT REQUIREMENT

*Lauren E. Babst**

Cite as: Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data with a Warrant Requirement*, 21 MICH. TELECOMM. & TECH L. REV. 363 (2015).
This manuscript may be accessed online at repository.law.umich.edu.

ABSTRACT

In modern society, the cell phone has become a virtual extension of most Americans, managing all kinds of personal and business matters. Modern cell tower technology allows cell service providers to accumulate a wealth of individuals' location information while they use their cell phones, and such data is available for law enforcement to obtain without a warrant. This is problematic under the Fourth Amendment, which protects reasonable expectations of privacy. Under the Katz two-prong test, (1) individuals have an actual, subjective expectation of privacy in their cell site location data, and (2) society is prepared to acknowledge that expectation as reasonable. In addtion, I propose that the second prong of the Katz test should be approached as a normative inquiry. Courts should ask whether society should expect privacy in this type of information. Currently, courts analyzing this issue have followed Supreme Court precedent from the 1970s and 80s, using shortcuts such as the third-party doctrine to decide the issue. This precedent is from an era that predates modern cell phone technology, and it fails to properly address the true privacy concerns implicated by cell site location data. A few courts have adopted the mosaic theory approach to the question of cell site location data. However this theory also fails to effectively guard against unconstitutional government intrusion in all instances. I propose that the best solution is to always require a warrant before allowing law enforcement to access cell site location data. This solution will provide a clear standard for courts, individuals, law enforcement agents, and cell service providers; also, it will ensure

* J.D., University of Michigan, 2016 (expected); B.A., English and Political Science, University of Michigan, 2012. Special thank you to Professor Susan Freiwald for her expert insight and guidance and to Micah Siegel Wallace for his valuable contributions and editorial assistance. I also thank Parker Lee for his thought-provoking arguments, and my friends and family for their support.

that millions of innocent Americans are protected from intrusive government surveillance.

INTRODUCTION 364
I. THE CURRENT STATE OF LEGAL AFFAIRS 367
A. *Stored Communications Act* 368
B. *Federal Circuit Split* 369
II. MODERN CELL PHONE TCHNOLOGY PROVIDES A MEANS FOR INTRUSIVE GOVERNMENT SURVEILLANCE 371
A. *The Technology behind CSLI* 372
B. *Government Requests for CSLI* 373
C. *Disconnect between Service Provider Incentives and Individuals' Privacy Interests* 374
D. *Precision of CSLI as a Surveillance Tool* 375
III. THE FOURTH AMENDMENT PROTECTS REASONABLE EXPECTATIONS OF PRIVACY 376
A. *Subjective Expectations of Privacy in CSLI* 377
B. *Objective Expectations of Privacy in CSLI: A Normative Approach* 379
1. Supreme Court Support for a Normative Approach 380
2. Courts Adopting a Normative Approach 381
3. Statutory Provisions Suggest Special Protection for CSLI 383
4. Normative Considerations Demand a Warrant Requirement for CSLI 384
IV. THE THIRD-PARTY DOCTRINE DOES NOT APPLY TO CSLI 385
A. *CSLI is Not an Ordinary Business Record* 386
B. *CSLI is Analogous to Content* 388
C. *Cell Phone Users Do Not Voluntarily Convey Their Location Information* 390
V. THE MOSAIC THEORY SWALLOWS THE PUBLIC/PRIVATE DISTINCTION 393
A. *Development of the Mosaic Theory* 394
B. *The Mosaic Theory Fails to Adequately Protect CSLI* 395
VI. A JUDICIAL SOLUTION IS NEEDED TO PROTECT CELL PHONE USERS' LEGITIMATE EXPECTATION OF PRIVACY IN CSLI 397
CONCLUSION 399

INTRODUCTION

The pervasiveness of cell phones in modern society has presented new concerns for individuals' privacy and forced courts to decide whether Fourth Amendment protections should apply to the data that cell phones generate. Today, using a cell phone means that cell service providers can track individuals' physical location and store massive amounts of their location information. The Supreme Court has not yet decided the question of how courts should treat this data under the Fourth Amendment. Because this location data provides law enforcement with a powerful new method of investigation,

courts must choose whether to follow Supreme Court Fourth Amendment precedent from an era before modern cell phones,[1] or instead consider what legal standards should apply in light of the dramatic changes in technology.

Generally, cell site location information ("CSLI") is divided into two categories, historical data and real-time (or "prospective") data. Historical data is past location data accumulated over time and stored by the cell service provider, while real-time data is present data used to deduce the current location of the cell phone. The Electronic Communications Privacy Act of 1986 ("ECPA")[2] addresses real-time data in a separate section than historical data, which falls under the Stored Communications Act ("SCA").[3] The SCA authorizes the government to obtain customer service records from providers of electronic communications by obtaining a court order under 2703(d).[4] While courts considering real-time or prospective CSLI have generally held that the Fourth Amendment requires law enforcement to obtain a warrant before gaining access to such data,[5] courts have been slow to grant historical CSLI the same protections. However, ECPA was enacted well before modern cell phone technology, and the fact that it allows a lower standard for agents to acquire stored records "should carry little or no weight" on the issue of CSLI.[6]

---

1. Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012) (criticizing how "courts often fall back on the rules . . . from an earlier technological era" in applying the Fourth Amendment to surveillance technologies).

2. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986).

3. 18 U.S.C. § 2703 (2012).

4. 18 U.S.C. § 2703(c)–(d) (2012).

5. *See, e.g.*, United States v. Ruby, No. 12-CR-1073 WQH, 2013 WL 544888, at *4–6 (S.D. Cal. Feb. 12, 2013); United States v. Graham, 846 F. Supp. 2d 384, 405–06 (D. Md. 2012); United States v. Gordon, No. 09-153-02 (RMU), 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *2 (N.D. Ga. Apr. 21, 2008); *In re* U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers, 416 F. Supp. 2d 390, 397 (D. Md. 2006); *see also 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. 84 (2010) (statement of Stephen W. Smith, U.S. Mag. J.) ("Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information."). Some courts have allowed access to real-time or prospective cell site location data without a warrant, generally requiring the government to obtain a "hybrid order," which consists of an order under § 2703(d) as well as a pen register order under 18 U.S.C. § 3123. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 698–99 (2011).

6. Freiwald, *supra* note 5, at 738; *see* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 877 (2014)("In the intervening twenty-eight years, Congress has not meaningfully updated the SCA's records access provisions, let alone clarified whether they apply to location records."). A group of major technology companies, nonprofit organizations, civil liberties groups, and academics have formed the Digital Due Process

This Note will focus on historical CSLI and why it deserves Fourth Amendment protection, however, much of the analysis applies to CSLI generally. From a Fourth Amendment perspective, there is no "material difference" between historical and real-time CSLI, as the acquisition of either type implicates the same reasonable expectations of privacy.[7] The privacy interests that are implicated by government access to this data are not "meaningfully diminished" by a mere delay in disclosure.[8] Jurisdictions that require a warrant for real-time and not historical CSLI are leaving a loophole for law enforcement agents, where they may take advantage of the distinction and apply for instantaneously created "records" on an ongoing basis, calling it *historical* CSLI.[9] This loophole allows agents to completely circumvent the warrant requirement.[10] Many courts have recognized that the privacy concerns are the same in historic and real-time tracking cases,[11] and scholars

---

Coalition and recommended that Congress amend ECPA to remove distinctions between the treatment of historical and forward-looking data. *See* DIGITAL DUE PROCESS, http://www.digitaldueprocess.org (last visited Apr. 6, 2015).

7. *In re* Applications of the U.S. for Orders Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Info. & Historical Cell Site Info. for Mobile Phone Identification Nos: (XXX) XXX-AAAA, (XXX) XXX-BBBB, & (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 76 (D. Mass. 2007) (finding no "material difference" between "real time," prospective, and historical tracking), *reversed*, 509 F. Supp. 2d 76 (D. Mass. 2007); *see also* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 61–76 (2007) (arguing that stored data implicates reasonable expectations of privacy as much as forward-looking data unless it is isolated to a single point in time); *Our Principles*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163 (last visited Apr. 6, 2015) ("The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.").

8. *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008), *affirmed*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010)[hereinafter *Third Circuit Opinion*].

9. *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1034 (refusing to allow the Government to convert an application for real time CSLI into one for historical CSLI by claiming that the provider held the records briefly before delivering them); *In re* Application of U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 6:08-6038M-REW, 2009 WL 8231744, at *10 n. 15 (E.D. Ky. Apr. 17, 2009) (calling the government's attempts to obtain "freshly-created records" of location data as an "end-run around the legal limits on real-time access" and a "misuse of the SCA").

10. *See* Freiwald, *Light*, *supra* note 6, at 896–97 ("The government's ability to take advantage of the lower protection for historical data as compared to real-time location data adds urgency to the question of whether the two types of data should be treated the same in any case.").

11. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cellsite Info., 736 F. Supp. 2d 578, 585 (E.D.N.Y. 2010) (arguing that the fact that information is stored "says nothing about whether its creator has a reasonable expectation of privacy in that information"); *id.* ("The picture of Tyshawn Augustus's life the government seeks to obtain is no less intimate simply because it has already been painted."); *see also In re* United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010) *vacated*, *In re* U.S. for

agree that historical CSLI, "by virtue of creating a target's complete digital profile," should be protected by the Fourth Amendment.[12]

In Part I of this Note, I will introduce the problematic statutory standard of ECPA and the SCA, and summarize the split holdings of the Federal Circuit Courts. In Part II, I will introduce the mechanics of CSLI and the scope of government requests for such information, as well as the practices of service providers and the precision of CSLI as a surveillance tool. In Part III, I will conduct a Fourth Amendment analysis under the *Katz* test to show that individuals maintain a subjective expectation of privacy in CSLI and this expectation is recognized by society as objectively reasonable. Furthermore, I propose that the objective prong of the *Katz* analysis should be approached as a normative inquiry—courts should ask whether CSLI is the type of information that *should* be protected by a warrant requirement. In part IV, I will discuss how the third-party doctrine does not apply to CSLI because the criteria for applying the doctrine are absent in the context of CSLI. In part V, I will discuss how the mosaic theory has swallowed up the public/private distinction from past Fourth Amendment jurisprudence, and explain that the mosaic theory is also inappropriate for resolving the privacy concerns presented by CSLI. In part VI, I will propose judicial and legislative solutions, emphasizing the necessity for courts to act soon to protect Americans' privacy. The conclusion of this Note underlines the need for a warrant requirement in order to preserve the fundamental principle of the Fourth Amendment—to keep Americans protected from intrusive government surveillance.

I. The Current State of Legal Affairs

Law enforcement agents can use a court order under section 2703(d) of the SCA to obtain individuals' CSLI from cell service providers. Courts interpreting section 2703 have reached different conclusions as to whether this statute governs CSLI and, if it does, what protections it affords this data. The Third, Fifth, and Eleventh Circuit courts have all decided the issue differently, leaving desperate need for a clear standard regarding what Fourth Amendment protections apply to CSLI.

Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (emphasis added)[hereinafter *Fifth Circuit Opinion*] ("The temporal distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same, whether the tracking covers the previous 60 days or the next."). Tracey v. State, No. SC11-2254, 2014 WL 5285929 at *17 (Fla. Oct. 16, 2014), *reh'g denied* (Dec. 8, 2014) (citing a case addressing historical CSLI and concluding the "same principle applies here, where real time cell site location information used for tracking is at issue").

12. Freiwald, *supra* note 5, at 739–40; *see also* Stephen E. Henderson, *Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. Crim. L. & Criminology 803, 831 (2013).

A. *Stored Communications Act*

The Stored Communications Act, passed as part of ECPA, addresses communications records generally but never includes the words "historical" or "cell site."[13] Some courts have determined historical CSLI is outside the scope of the SCA, because the SCA is limited to information pertaining to wire or electronic communications, and those terms are defined to exclude communications from a device "which permits the tracking of the movement of a person or object."[14] Such courts reason that the government's use of CSLI characterizes the phone as a tracking device, and therefore the government is required to obtain a warrant.[15] Other courts, which have determined or assumed that historical CSLI falls under the SCA, have found the statute to be unclear and reached different conclusions about what procedural requirements the government must meet in order to obtain historical CSLI.[16]

Sections 2703(a) and (b) of the SCA address circumstances in which a governmental entity may require providers to disclose the *contents* of wire or electronic communications.[17] Here, the term "contents" is commonly understood to refer to the communicated message.[18] The statute generally requires law enforcement agents to make a showing of probable cause and obtain a warrant to acquire the contents of communications.[19] Some courts have characterized historical CSLI as "content" and found it should be protected by a warrant requirement on that basis.[20] On the other hand, sections 2703(c) and (d) address the *records* of a customer's use of electronic communications services; the term "records" is generally understood to refer to information about the communication that the service provider uses to process and de-

13. *In re* Application of the U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889 (S.D. Tex. 2014).

14. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 601 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, *Third Circuit Opinion*, *supra* note 8.

15. *Id.* at 607 (stating that CSLI is "expressly placed outside the scope of the electronic communications legislation of the SCA" and requiring government agents to meet probable cause standard); *see also*, *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("[P]ermitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns.").

16. *See, e.g.*, *Third Circuit Opinion*, *supra* note 8; *Fifth Circuit Opinion*, *supra* note 11, at 615 (emphasis added).

17. 18 U.S.C. § 2703(a)–(b) (2012) (emphasis added).

18. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 (2004) ("Content information is the communication that a person wishes to share or communicate with another person.").

19. 18 U.S.C. § 2703(a)(2012)(The statute includes a series of complicated distinctions allowing access to some content without a warrant, but such distinctions are beyond the scope of this Note.); *id.* at (b).

20. See section IV.B on CSLI as analogous to content information.

liver the message.[21] The statute requires law enforcement agents to present "specific and articulable facts showing that there are reasonable grounds to believe" the records are "relevant and material to an ongoing criminal investigation" in order to obtain a court order for disclosure of service providers' records under § 2703(d).[22]

Because the standard to acquire records is a much more lenient standard, the government can gather much more information than a probable cause standard would permit.[23] Under the probable cause standard, the information sought must itself be evidence of a crime.[24] Under the 2703(d) standard, however, law enforcement need only show the information sought is "relevant and material to an ongoing investigation."[25] Also, there is no statutory limit on the scope of the historical CSLI the government may request. The only limit is the "length of time a target's cell phone generates records and the service provider stores them."[26] The government has been exploiting this lower 2703(d) standard to conduct wide-ranging inquiries, gathering massive amounts of CSLI for large numbers of cell phone users at a time.[27]

B. *Federal Circuit Split*

Federal appellate courts are split as to whether a warrant is required for historical CSLI, suggesting the Supreme Court needs to make a definitive ruling. The Third Circuit found that law enforcement agents may obtain historical CSLI through a 2703(d) court order without violating the Fourth

---

21. *See* Kerr, *supra* note 18, at 1228 ("[N]oncontent information . . . is information about the communication that the network uses to deliver and process the content information.").

22. 18 U.S.C. § 2703(c)–(d)(2012).

23. Freiwald, *supra* note 5, at 698; *see also Third Circuit Opinion*, *supra* note 8, at 315 (stating that the "reasonable grounds to believe" standard for a 2703(d) order is "less stringent than probable cause"); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("This showing is lower than the probable cause standard required for a search warrant.").

24. *See*, *e.g.*, *In re* U.S. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (noting a difference in the standards because probable cause requires a finding that the information sought is itself evidence of a crime rather than relevant and material to the investigation).

25. 18 U.S.C. § 2703 (2012).

26. Freiwald, *supra* note 5, at 698; *see*, *e.g.*, United States v. Davis, No. 12-12928, 2014 WL 6526854, at *1 (11th Cir. Nov. 15, 2014) (en banc) (stating the case involved the disclosure of 67 consecutive days of cell tower site data, and the government, in seeking an order to compel disclosure, asserted only that seven days of cell site data met the relevance and materiality test).

27. Catherine Crump & Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 CRIM. L. REP. 19, 5 (2010) (describing a recent case in which the FBI sought and received tracking information, without a warrant, for 180 people in addition to the criminal defendant). *see* section II-B on the nature of government requests.

Amendment.[28] It cautioned, however, that agents are "not free from the warrant requirement"[29] under the SCA, because historical CSLI may, in certain circumstances, reveal private information protected by the Fourth Amendment.[30] The court decided the statute allows a Magistrate Judge to use their discretion to require a warrant to obtain historical CSLI.[31] This holding places a significant burden on Magistrate Judges to conduct a balancing test without any clear instruction as how to administer it.[32]

Handling the question differently, the Fifth Circuit found that CSLI falls under the Supreme Court line of precedent holding that an individual's records stored by a third party in their ordinary course of business are not protected by the Fourth Amendment.[33] The court held that § 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."[34] The court also differed from the Third Circuit by holding that the magistrate judge has no discretion to deny the Government's application for a § 2703(d) order that meets the statutory requirements.[35] However, the court was careful to note that the holding applied only to the "narrow issue" before them,[36] and admitted "specific orders [for CSLI] may be unconstitutional because of additional facts involved in the case."[37] Therefore the Fifth Cir-

28. *Third Circuit Opinion*, *supra* note 8, at 319. It is worth noting that the Third Circuit decided the issue before the Supreme Court issued its opinion in *United States v. Jones*, which the Eleventh Circuit refers to as "the most instructive Supreme Court decision in the field." United States v. Davis, 754 F.3d 1205, 1212 (11th Cir. 2014) [hereinafter *Eleventh Circuit Opinion*], *vacated*, 573 F. App'x 925 (11th Cir. 2014).

29. *Third Circuit Opinion*, *supra* note 8, at 318.

30. *See id.* at 312 ("The *Knotts*/*Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home. There is no evidence in *this* record that historical CSLI. . . extends to that realm."); *see also id.* at 320 (Tashima, J., concurring) ("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 under § 2703(d) 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.").

31. *Id.* at 319 (majority opinion) (remanding the case to the magistrate judge to decide if a warrant should be required rather than a § 2703(d) order).

32. Freiwald, *Light*, *supra* note 6, at 889; *see Third Circuit Opinion*, *supra* note 8, at 319 ("[W]e are stymied by the failure of Congress to make its intention [regarding whether to require a warrant] clear."); *id.* at 320 (Tashima, J., concurring) (complaining that the majority's interpretation "provides no standards for the approval or disapproval for an application for an order under § 2703(d)"); *see also* Stephen W. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. Rev. 257, 262 (2012) ("So despite a pressing need for appellate court guidance to magistrate judges deluged with [ECPA] requests on a daily basis, almost none has been given.").

33. *Fifth Circuit Opinion*, *supra* note 11, at 615 (emphasis added)

34. *Id.* (emphasis added).

35. *Id.*

36. *Id*.

37. *Id.* at 614

cuit case also fails to offer guidance to lower courts as to when they should require a warrant to obtain historical CSLI.[38]

The Eleventh Circuit decided the issue differently from both the Third and Fifth Circuits, holding that historical CSLI is within an individual's reasonable expectation of privacy and that obtaining such data without a warrant is a Fourth Amendment violation.[39] This holding offers a clear and workable standard for lower courts to apply and for the government to follow. The Eleventh Circuit's opinion, however, has been vacated and is currently scheduled for a rehearing en banc. The Fourth Circuit is also currently considering the question on appeal.[40] This state of affairs has left lower courts, service providers, and individuals uncertain as to what Fourth Amendment protections are afforded to CSLI. The constitutional question is ripe for review by the Supreme Court, and the answer is simple: require a warrant.

II. Modern Cell Phone Tchnology Provides a Means for Intrusive Government Surveillance

Today, it is estimated that more than 90 percent of American adults own a cell phone.[41] Many people treat their cell phones as a "virtual extensions" of themselves, "using them for all manner of necessary and personal matters."[42] Even the Supreme Court has recognized that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[43] Cell phones are constantly generating and automatically sending a wealth of location information to cell service providers who, in turn, store

38. *See* Freiwald, *Light*, *supra* note 6, at 889 ("The Fifth Circuit's approach covers a small subset of location data and gives little direction about the vast amount of data it leaves unaddressed.").

39. *Eleventh Circuit Opinion*, *supra* note 28, at 1217.

40. *See* United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012) (appeal currently pending before the Fourth Circuit). Defendant Aaron Graham filed an appeal with the Fourth Circuit, challenging the district court's ruling. Oral arguments took place on December 11, 2014 (Fourth Circuit schedule *available at* http://pacer.ca4.uscourts.gov/calendar/internetcaldec092014ric.pdf).

41. *Mobile Technology Fact Sheet*, Pew Research Center (January 2014), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet.

42. Tracey v. State, 152 So. 3d 504 (Fla. 2014).; *see also* Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."); *see also In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("For many Americans, there is no time in the day when they are more than a few feet away from their [cellular telephones].").

43. *Riley*, 134 S. Ct. at 2484, 2490 (2014).

this information.[44] Because cell phone users usually keep their cell phone on or near their person, this information reveals their location at any given time.

A. *The Technology behind CSLI*

Cell phones operate by sending signals to transmitting stations known as cell "sites" or "towers" which are strategically placed throughout the service provider's network.[45] When a cell phone is on, it will automatically register and identify with the nearest tower or the one with the strongest signal.[46] The cell phone automatically re-scans every seven seconds, or whenever the signal strength weakens, to make connections with cell sites.[47] This automatic identification is referred to as registration data. When a cell phone places or receives a call, the phone must communicate with nearby cell towers to determine which tower will handle the call.[48] Initiation data indicates the nearest cell tower (or towers) to the cell user when a call begins, and termination data refers to such data created when the call ends.[49] There is also duration data, which includes a record of all the transmissions between the cell phone and the nearest cell site(s) during a phone call.[50]

The specificity with which CSLI can track a user depends on the proximity of cell sites, which vary by provider and location.[51] Cell sites are generally built much closer to each other in urban areas due to the considerably higher volume of calls in such areas. According to a recent Cellular Telecommunications Industry Association study, the number of cell sites in the U.S. has almost tripled in the last ten years.[52] Cell service providers are constructing "ever denser networks"[53] to keep pace with the "explosive growth" in the demand for wireless technology.[54] In addition, service providers must "comply with federal regulations requiring them to provide emergency dispatchers with increasingly precise coordinates for 911 calls placed

---

44. Commonwealth v. Augustine, 4 N.E.3d 846, 860 (Mass. 2014).

45. *See generally 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. 20 (2010) (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania).

46. *See generally Id.*

47. *See* State v. Earls, 70 A.3d 630, 643 (N.J. 2013); *See also In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

48. Freiwald, *supra* note 5, at 702–03

49. *Id.* at 703.

50. *Id.* at 704–05.

51. *See generally ECPA Reform supra*, note 45 (statement of Matt Blaze).

52. *See Semi-Annual Wireless Industry Survey*, CTIA-The Wireless Ass'n, at 2, http://files.ctia.org/pdf/CTIA__Survey_Midyear_2010_Graphics.pdf (reporting that the number of cell sites in service increased forty percent in the last five years and had almost tripled in the last ten years)

53. *Fifth Circuit Opinion*, *supra* note 11, at 630 (Dennis, J., dissenting).

54. *ECPA Reform supra*, note 45 (statement of Matt Blaze).

by cell phone."[55] This has led to the development of new cell site technology which can pinpoint an individual's location in very small areas, such as "particular floors of buildings or even individual home and offices."[56] Analysts can use triangulation methods on data from overlapping cell towers to find a phone's location at a level of accuracy approaching that of GPS technology.[57]

B. *Government Requests for CSLI*

By obtaining historical CSLI, the government can figure out a suspect's location both at a particular time and across long periods of time to determine places an individual frequently visits and map their common routes. Law enforcement requests for this information regularly include disclosure of location data of seemingly innocent parties.[58] Agents often request disclosure of *all* calls handled by a particular cell tower in a "community of interest,"[59] or request the location data of "all of the associates who called or made calls to a target."[60] Allowing law enforcement agencies to enjoy warrantless access to this information leaves more than 335 million Americans at risk of surveillance.[61]

What is especially problematic is that courts may rely "at their peril" on government representations about the limits of the location data they seek.[62] In the case before the Third Circuit, the Government's application for historical CSLI of a particular cell phone requested, "without limitation," call ini-

---

55. *Fifth Circuit Opinion*, *supra* note 11, at 630 (Dennis, J., dissenting) (citing 911 Service, 47 C.F.R. § 20.18(h)(1)).

56. *ECPA Reform supra* note 45 (statement of Matt Blaze) (discussing the invent of "microcells", "picocells" and "femtocells").

57. *Id.* at 26; *see also* Stephanie Lockwood, *Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 312 (2004) ("The reality that people carry their cell phones on their persons means that cell phone tracking technology potentially offers a detailed view of a given subscriber's movements rather than simply providing call-identifying information.").

58. Crump, *supra* note 27, at 6 ("[I]t appears that the government took the dragnet approach of getting location information for a large number of innocent people to try to figure out who was involved in the crime.").

59. *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29–30 (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP) (describing a common practice of government agents seeking the "location [information] of the community of interest—that is, the location of persons with whom the target communicates")

60. Albert Gidari, Jr., *Keynote Address: Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 557 (2007).

61. *See Annual Wireless Industry Survey*, CTIA-THE WIRELESS ASS'N, at 2, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (As of December 2013, there were 335.65 million wireless subscriber accounts in the United States, responsible for 2.61 trillion annual minutes of calls and 1.91 trillion annual text messages.).

62. Freiwald, *supra* note 5, at 708.

tiation and termination data, duration data, and registration data.[63] However, the government represented in its papers that it sought only initiation, duration, and termination data.[64] This is a drastic discrepancy, as registration data shows the cell phone's location at least every seven seconds and provides immensely more information. The government at oral argument further misrepresented its application to the court, stating that it sought only initiation and termination data and not registration or duration data.[65] While this is only one example, it suggests a larger issue that the government may not be accurately describing, and courts not accurately assessing, the gravity of the invasion of privacy in CSLI cases. The Fifth Circuit recognized this difference and was careful to note that its holding did not apply to orders requesting duration or registration data.[66] Because of the ex parte and sealed nature of the government's requests, it is impossible to know whether other courts have been misled as to the scope of government requests for CSLI.[67]

C. *Disconnect between Service Provider Incentives and Individuals' Privacy Interests*

Further exacerbating the problem is the fact that cell service providers may not necessarily limit the records they furnish to the government to the exact information requested. The interests of the service provider may not align with an individual's privacy interests, as profit motives can "impel providers to make disclosure decisions based on the lowest cost rather than to decide based on the best interests of the target."[68] Considering the scope of the service provider's records, "there would be neither reason nor way for providers to filter the data in order to deliver only limited data."[69] The information conveyed to the government can include "duration, registration, triangulation, and GPS data, all of which can provide an extremely rich and

63. *Third Circuit Opinion*, *supra* note 8, at 308 (citing App. at 64 and quoting from the "heavily redacted" application to the Magistrate Judge.).

64. *See* Gov't Reply Brief at 6, *Third Circuit Opinion*, *supra* note 8, (No. 08-4227) (citing the exemplar submitted to the district court as proof that the information sought by the government is limited to date, time, telephone number, the cell tower used to connect to the call, the cell tower used at the end of the call, and the duration of the call).

65. *See* Oral Argument at 35:06–36:19, *Third Circuit Opinion*, *supra* note 8, available at www.ca3.uscourts.gov/oral-argument-recordings, file 08-4227-ApplicationofUSA.wma (arguing that location data in the exemplar was recorded only when calls were started or ended and points out that the exemplar did not include registration data).

66. *Fifth Circuit Opinion*, *supra* note 11, at 615.

67. Freiwald, *supra* note 5, at 717–18.

68. *Id.*

69. *Id.*; *see also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1010–13 (1996) (questioning the calculation that equates service provider interests with subscribers' privacy interests, particularly when subscribers will not find out about disclosures).

precise picture of a target's movements" and the government "will likely receive more information than they request."[70]

In fact, the number of requests that service providers receive on a daily basis is incredibly burdensome. As AT&T explained in its amicus brief for the Eleventh Circuit rehearing en banc, it had to create a separate center that operates on a continuous basis just to respond to judicial orders and subpoenas.[71] AT&T asked the court to announce a categorical standard for all government orders seeking historical CSLI, so that clear rules can be set for law enforcement agents, lower courts, and service providers to ensure they are able to protect legitimate privacy concerns and law enforcement interests.[72]

D. *Precision of CSLI as a Surveillance Tool*

The Government often argues, as shown in *Davis*, that CSLI should be less protected than GPS data because it is "less precise."[73] The Eleventh Circuit expressly rejected this argument, rationalizing that "the information is sufficiently specific that the prosecutor expressly relied on it in summing up to the jury."[74] The fact that CSLI may in some instances fall short of the precision of GPS data does not necessarily mean it prevents law enforcement from tracking an individual's physical movements. As the Third Circuit stated: "even imprecise information, when combined with visual surveillance or a known address, can enable law enforcement to infer the exact location of a phone."[75] The government routinely uses CSLI this way. Moreover, the government has advised juries in various cases that it "should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home."[76] Even the Fifth Circuit admitted that "the reason the Government seeks such information is to locate or track a suspect in a criminal investigation" and that "[t]he data must be precise enough to be useful to the Government, which would suggest that, at least in some cases, it can narrow someone's location to a fairly small area."[77] Any

70. Freiwald, *supra* note 5, at 718.

71. Brief for AT&T as Amici Curiae Supporting Neither Party at 2–3, United States v. Davis, 573 F. App'x 925 (11th Cir. 2014) (en banc) (No-12-12928). AT&T's center employs more than 100 full time employees, and for the first half of 2014, the center processed nearly 116,000 requests for various types of information.

72. *Id.* at 30

73. *Eleventh Circuit Opinion*, *supra* note 28, at 1216 (11th Cir.), *vacated,* 573 F. App'x 925 (11th Cir. 2014).

74. *Id.*

75. Brief for ACLU as Amici Curiae Supporting Defendant-Appellant at 15, United States v. Davis, 573 F. App'x 925 (11th Cir. 2014) (en banc) (No-12-12928).

76. *Third Circuit Opinion*, *supra* note 8, at 311–12

77. *Fifth Circuit Opinion*, *supra* note 11, at 609.

difference in precision between CSLI and GPS does not have "constitutional significance."[78]

Not to mention, the argument that CSLI is imprecise is contradicted by the statements of experts in the field of modern cell phone technology who compare it favorably to GPS-technology in some cases. Matt Blaze, an Associate Professor of Computer and Information Science at the University of Pennsylvania, said the following in his statement to Congress:

> As the precision provided by cellular network-based location approaches that of GPS-based tracking technology, cellular location tracking can have significant advantages for law enforcement surveillance operations compared with traditional GPS trackers. New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cell phone location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the subject. And the 'tracking device' is now a benign object already carried by the target – his or her own telephone.[79]

This information proves that CSLI cannot be compared to information obtained by "a policeman following someone on a public street," because to make such a claim would be to "fundamentally misunderstand the richness of [CSLI] and the power of its use as a surveillance tool."[80] CSLI provides a precise and comprehensive record of a cell phone user's movements at virtually any time day, whether they are in public or private, and the government should have to show probable cause before accessing such sensitive information.

III. The Fourth Amendment Protects Reasonable Expectations of Privacy

The Fourth Amendment guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[81] The government conducts a search within the meaning of the Fourth Amendment when it "violates a subjective expectation of privacy that society recognizes as reasonable."[82] Justice Harlan first articulated this standard in 1967 in his concurring opinion in *Katz v. United States*,

78. *Eleventh Circuit Opinion*, *supra* note 28, at 1216 ("[The fact that] information obtained by an invasion of privacy may not be entirely precise does not change the calculus as to whether obtaining it was in fact an invasion of privacy.").

79. *See ECPA Reform*, *supra* note 45 (statement of Matt Blaze).

80. Freiwald, *supra* note 5, at 709.

81. U.S. Const. amend. IV.

82. Kyllo v. United States, 533 U.S. 27, 33 (2001).

and the Supreme Court has since used it repeatedly when considering alleged Fourth Amendment violations.[83]

The Fourth Amendment protects an individual's reasonable expectation of privacy and its protections apply to emerging cell phone technology. The Supreme Court has recognized that permitting the government to exploit new technology would "erode the privacy guaranteed by the Fourth Amendment."[84] The reasonableness of an individual's expectation of privacy must be determined in light of technological progress, because it would be an "Orwellian notion" to assume that "previous liberties derived from the Framers simply shrink as the government acquires new means of infringing them."[85] Indeed, "it hardly makes sense to read *Katz* as meaning that we assume the risk of whatever technology the government can bring to bear upon its investigative efforts."[86] There is a reasonable expectation of privacy in CSLI, and the government obtaining such data constitutes a search under the Fourth Amendment. It is a basic principle of Fourth Amendment law that searches and seizures without a warrant "are presumptively unreasonable," with only a few limited exceptions.[87] None of these exceptions apply to CSLI, partially because of its unique nature, and therefore warrantless access to historical CSLI constitutes an unreasonable search in violation of the Fourth Amendment.

A. *Subjective Expectations of Privacy in CSLI*

As Justice Stevens stated: "As a general matter, the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices."[88] Most Americans have no idea that cell service providers store vast amounts of CSLI and allow the government warrantless access to it.[89] This was illustrated in 2011, when consumers learned that iPhones stored ten months of location data in an unencrypted format; the rapid influx of consumer complaints led Apple to revise its entire iPhone operating system within a week to protect consumers' location infor-

83. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see, e.g.*, *Kyllo*, 533 U.S. at 27; United States v. Karo, 468 U.S. 705, 712 (1984).

84. *Kyllo*, 533 U.S. at 34.

85. People v. Cook, 710 P.2d 299, 305 (Cal. 1985); *see also Kyllo*, 533 U.S. at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

86. Wayne LaFave, *The Forgotten Motto of Obsta Principiis in Fourth Amendment Jurisprudence*, 28 ARIZ. L. REV. 291, 307 (1986).

87. *See, e.g.*, Groh v. Ramirez, 540 U.S. 551, 559 (2004).

88. *Karo*, 468 U.S. at 735 (Stevens, J., concurring in part and dissenting in part).

89. *See* Freiwald, *supra* note 5, at 743 ("Most cell phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their location information without first obtaining a warrant based on a showing of probable cause.").

mation.[90] Cell phone users maintain their expectation of privacy in their location information, because they cannot assume the risk of disclosure if they are not even aware that this information is being shared.[91] People expect law enforcement agents to obtain a warrant before bugging individuals' phones and monitoring their calls, and for the same reason, people expect such a requirement before law enforcement agents can use individuals' cell phones to track their movements for any period of time.[92]

Research shows that Americans expect privacy in their CSLI. In November 2014, the Pew Research Center found that 82 percent of American adults considered data showing the details of their physical location over time to be sensitive information—more sensitive than the content of their text messages, their relationship history, their web browser history, their religious views, or their political views.[93] Similarly, a 2008 research report showed that 73 percent of cell phone users responded that they favored requiring "the police to convince a judge that a crime has been committed before obtaining historical location information from the cell phone company."[94] The report also showed that 72 percent of respondents supported a law requiring police to give notice to the cell user before they may obtain historical records of location data.[95] Also, the Pew Research Center found in 2012 that cell phone users take a number of steps to protect their personal information and mobile data, showing that more than half of cell users have chosen to uninstall or not install an app due to concerns about maintaining the privacy of their personal information.[96] This research shows cell phone users are far from comfortable with sharing their location information, and

---

90. Press Release, Apple, Inc., Apple Q&A on Location Data (April 27, 2011) (available at https:// www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html).

91. *Fourth Amendment - Warrantless Searches - New Jersey Supreme Court Holds That State Constitution Requires Police to Obtain Warrant Before Accessing Cell-Site Location Information*, 127 HARV. L. REV. 2164, 2169 (2014) [hereinafter *Fourth Amendment*]; *See Third Circuit Opinion*, *supra* note 8, at 317–18.

92. *See* Freiwald, *supra* note 5, at 744–45 ("For the same reasons that people expect a law enforcement agent to obtain a warrant from a neutral magistrate before he may bug their conversations, monitor their phone calls, or subject them to silent video surveillance, people would surely expect judicial oversight of an agent's use of their cell phones to track their movements and activities.").

93. Mary Madden, PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA, 36–37 (Nov. 2014), *available at* http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (50% of American adults consider their location information to be "very sensitive").

94. Jennifer King & Chris Jay Hoofnagle, Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information 8–9 (Apr. 18, 2008)(unpublished manuscript), *available at* http://ssrn.com/abstract=1137988.

95. *Id.* at 8.

96. Jan Lauren Boyles, Aaron Smith, and Marry Madden, PEW RESEARCH CENTER, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES, (Sept. 5, 2012), *available at* http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

they are certainly against law enforcement agents using individuals' cell phones to track their every movement.[97]

Even with all this subjective evidence, the focus of a court's Fourth Amendment analysis should be on the normative inquiry demanded by the second prong of the *Katz* test. Four years after enunciating the famous *Katz* test, Justice Harlan stated that a court's analysis must "transcend the search for subjective expectations or legal attribution of assumptions of risk,"[98] and he called for courts to conduct a normative inquiry.[99] The Supreme Court validated Harlan's view in *Smith v. Maryland*, stating that there are situations "where an individual's subjective expectations ha[ve] been 'conditioned' by influences alien to the well-recognized Fourth Amendment freedoms," and in such circumstances, a normative inquiry becomes necessary to determine whether a legitimate expectation of privacy exists.[100] In other words, when an individual lacks an actual expectation of privacy in something merely because he has experienced or been told that he lacks any privacy in it; courts should apply a normative analysis.[101]

B. *Objective Expectations of Privacy in CSLI: A Normative Approach*

The second prong of the *Katz* test is the determination of whether society recognizes the individual's subjective expectation of privacy as reasonable.[102] This prong requires courts to "make a normative finding about whether users *should* be entitled to view the object of the search as private."[103] Justice Harlan explained that the critical question for courts to assess is "whether, under our system of government, as reflected in the Constitution, we should impose on our citizens the risk of the electronic listener or observer without at least the protection of a warrant requirement."[104] Advances in technology certainly require special consideration because they implicate unique concerns for protecting individual's privacy.

97. *See* Stephanie Lockwood, *Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 316 (2004) ("[P]eople are likely to reject the prospect of turning every cell phone into a tracking device.").

98. United States v. White, 401 U.S. 745, 786–87 (1971).

99. *See id.* (Harlan, J., dissenting) ("This question must, in my view, be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement.").

100. Smith v. Maryland, 442 U.S. 735, 740 n. 5 (1979).

101. *See id.* ("For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects").

102. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

103. Freiwald, *supra* note 5, at 745.

104. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

The Supreme Court in *Riley v. California* emphasized that cell phones present novel privacy concerns as they store "qualitatively different" types of data than traditional physical records.[105] In order to properly analyze the scope of the privacy interests at stake, courts must account for the fact that modern technology can store vastly greater amounts of data and disclose much more revealing personal information than past technology.[106]

1. Supreme Court Support for a Normative Approach

There are five Supreme Court justices who, through concurring opinions in *United States v. Jones*, expressed concern over the particularly sensitive nature of location information and the implications that evolving technology will have on Fourth Amendment jurisprudence.[107] Justice Alito, in a concurring opinion joined by Justices Ginsburg, Breyer, and Kagan, recognized that "society's expectation has been that law enforcement agents and others would not [. . .] secretly monitor and catalogue every single movement of an individual's car for a very long period."[108] While *Jones* involved data gathered from a GPS device, Justice Alito elaborated in his opinion to discuss how recent developments in technology have led to the emergence of many new devices with tracking capabilities, and he specifically pointed to cell phones as the most significant development.[109] He also cautioned that use of these new devices would "continue to shape the average person's expectations about the privacy of his or her daily movements,"[110] suggesting that such new surveillance methods would shift the *Katz* analysis to focus on normative considerations.

Justice Sotomayor also made clear her concern about protecting location information, as she questioned the "appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercise of police power to [sic] and prevent 'a too permeating police surveillance.' "[111] Though expressed in the context of GPS surveillance, this concern applies equally to CSLI because it is a "tool so amenable to misuse" as demonstrated by the nature of government requests for such information.[112] In addition, Justice Sotomayor stated she would "not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment

105. Riley v. California, 134 S. Ct. 2473, 2490 (2014).
106. *Cf. id.* at 2491.
107. *See generally* United States v. Jones, 132 S. Ct. 945 (2012).
108. *Id.* at 964 (Alito, J., concurring).
109. *Id.*
110. *Id.*
111. *Id.* at 956 (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
112. *See supra* Part II-B (discussing the nature of government requests).

protection" because "whatever the societal expectations, [such expectations] can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[113] This shows that Justice Sotomayor would focus her analysis on the question of whether CSLI is the type of information that society *should* legitimately expect the Fourth Amendment to protect with a warrant requirement.

2. Courts Adopting a Normative Approach

Many federal and state courts addressing CSLI have adopted a normative approach to the objective prong of the *Katz* test and found that society is entitled to expect privacy in such information.[114] The Eleventh Circuit recognized that CSLI was "private in nature" because it could place someone "near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute," and found that individuals are entitled to have such information guarded by a warrant requirement.[115] Federal district courts reflected this sentiment, finding that to withhold Fourth Amendment protections from historical CSLI "would [be to] permit governmental intrusion into information which is objectively recognized as highly private."[116] These courts recognized that "[i]n light of drastic developments in technology, the Fourth Amendment doctrine must evolve" in order to preserve society's reasonable expectation of privacy in CSLI.[117]

---

113. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

114. *See*, *e.g.*, *Eleventh Circuit Opinion*, *supra* note 28, at 1217 (11th Cir.) *vacated*, 573 F. App'x 925 (11th Cir. 2014); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011); Tracey v. State, No. SC11-2254, 2014 WL 5285929 (Fla. Oct. 16, 2014), *reh'g denied* (Dec. 8, 2014); Commonwealth v. Augustine, 4 N.E. 3d 846 (Mass. 2014).

115. *Eleventh Circuit Opinion*, *supra* note 28, at 1216–17.

116. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011); *see also id.* at 119 ("[T]he collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip."); *see also In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010), *vacated*, *Fifth Circuit Opinion*, *supra* note 11 ("[Cell phone tracking] will also inevitably be more intrusive [than GPS tracking], because the phone can be monitored indoors where the expectation of privacy is greatest."); *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008), *vacated*, *Third Circuit Opinion*, *supra* note 8 (stating that Fourth Amendment protections depend on the "nature of the records or information sought").

117. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d at 127; *see also In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 845 ("[C]onsumers are not forced to sacrifice locational privacy as the price of using cell phones."); *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 595 (E.D.N.Y. 2010), *rev'd* (Nov. 29, 2010) ("[T]he Fourth Amendment's concept of an 'unreasonable' intrusion into one's personal affairs, by its very nature" must "evolve along with the myriad ways in which humans contrive to interact with one another.").

Several State Supreme Courts have also held that CSLI is private in nature and should be protected by the Fourth Amendment.[118] For example, the New Jersey Supreme Court held that cell phone users are "entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives," because cell phones are not meant to serve as tracking devices.[119] Following suit, the Massachusetts Supreme Court found that historical CSLI allows law enforcement to "track and reconstruct a person's past movements" to an extent that was never possible through traditional investigation methods.[120] The Florida Supreme Court confirmed that society is "now prepared to recognize" individual's expectations of privacy in CSLI as objectively reasonable under the *Katz* test.[121]

The Sixth Circuit opinion in *Warshak*, though it addressed stored e-mails, is also instructive in its emphasis on the need for a normative approach to the *Katz* analysis. The Sixth Circuit stated, "[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[122] The *Warshak* court reasoned that, because e-mail "plays an indispensable part in the Information Age," it requires strong Fourth Amendment protection; otherwise, the Fourth Amendment would be an "ineffective guardian of private communication, an essential purpose it has long been recognized to serve."[123]

Cell phones play an equally indispensable part in modern society, and the Fourth Amendment must recognize and protect the tremendous amounts of personal data this emerging technology generates. If the Fourth Amendment's protections were to narrow each time society became accustomed to their private information being acquired by law enforcement without a warrant, then surely as means of surveillance technology increase, constitutional protections will continue to be diminished, and eventually, cease to exist altogether.[124]

---

118. *Tracey*, 2014 WL 5285929; Commonwealth v. Augustine, 4 N.E. 3d 846 (Mass. 2014); State v. Earls, 70 A.3d 630, 644 (N.J. 2013). In New Jersey, there is no third-party doctrine, and the case was decided based on whether the government violated an individual's reasonable expectation of privacy. *See Earls*, 70 A.3d at 632.

119. *Earls*, 70 A.3d at 643 ("People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with the police"); *see also id.* ("[I]n 2006, cell phones could be tracked to within a one-mile radius or less of the nearest cell tower" and "that distance has narrowed to the point that cell phones can be pinpointed with great precision—to within feet in some instances").

120. *Augustine*, 4 N.E.3d at 865.

121. *Tracey*, 2014 WL 5285929 at *18–19.

122. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

123. *Id*.

124. *See supra* FN 99–101 about how individuals cannot have their Fourth Amendment rights conditioned by government intrusion.

3. Statutory Provisions Suggest Special Protection for CSLI

Courts should take into account Congressional intent in passing statutory protections for CSLI,[125] because an act of Congress affecting a proprietary interest is "undeniably relevant to the legitimate-expectation-of-privacy inquiry."[126] So far five states, Colorado, Maine, Minnesota, Montana, and Utah, have passed statutes requiring law enforcement to apply for a search warrant to obtain historical CSLI,[127] while several other state legislatures have recognized the threat to privacy and are still in the process of passing a warrant requirement.[128] In addition, numerous other states have passed laws requiring law enforcement to obtain a warrant before accessing real-time CSLI.[129] This shows a trend that society is increasingly recognizing the private nature of CSLI and demanding "the most scrupulous protection from government invasion."[130]

Furthermore, the Wireless Communication and Public Safety Act of 1999 ("WCPSA"),[131] which was enacted after the SCA and specifically addresses location data, "sends a strong signal to protect cell phone location data."[132] The WCPSA prohibits cell-service providers from disclosing "individually identifiable customer proprietary network information," including location data, except as required by law or with customer approval.[133] This suggests that Congress "intended individuals' privacy interest in location data be given particular weight in privacy assessments."[134] The WCPSA also

125. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010) ("state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable"); Doe v. Broderick, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection "is relevant to the determination of whether there is a 'societal understanding' that Doe has a legitimate expectation of privacy in his treatment records."); United States v. Nerber, 222 F.3d 597, 604–05 (9th Cir. 2000) (federal wiretap statute is "strong evidence" that society would find warrantless video surveillance unreasonable).

126. *In re* Application of U.S. for An Order Authorizing Release of Historical Cell-Site Data, 747 F. Supp. 2d 827, 842 (S.D. Tex. 2010) *vacated*, *Fifth Circuit Opinion supra* note 11.

127. *See* Colo. Rev. Stat. Ann. § 16-3-303.5(2) (West 2014); Me. Rev. Stat. tit. 16, § 648 (2014); Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2) (West 2014); Mont. Code Ann. § 46-5-110(1)(a) (2014); Utah Code Ann. § 77-23c-102(1)(a) (West 2014).

128. *See, e.g.*, S. 1052, 2013 Leg., 83d Reg. Sess. (Tex. 2013); *see also* Hanni Fakhoury, *New Massachusetts Decision Requires a Warrant for Cell Tracking*, Deeplinks Blog (Feb. 19, 2014), *available at* https://www.eff.org/deeplinks/2014/02/massachusetts-requires-warrants-cell-tracking (describing pending state bills to require warrants for location records). *But see* S. 1434, 2011–2012 Leg., Reg. Sess. (Cal. 2012) (vetoed by Governor on Sept. 30, 2012).

129. *See, e.g.*, Ind. Code Ann. § 35-33-5-12 (West 2014); Wis. Stat. Ann. § 968.373(2) (West 2014)

130. Oliver v. United States, 466 U.S. 170, 178 (1984).

131. Pub. L. No. 106-81, 113 Stat. 1286 (codified as amended in scattered sections of 47 U.S.C.).

132. *Fourth Amendment*, *supra* note 91, at 1227.

133. 47 U.S.C. § 222(c)(1), (h)(1) (2008).

134. *Fourth Amendment*, *supra* note 91, at 1226; *see In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 842 (S.D. Tex. 2010) *vacated*, *Fifth Circuit Opinion*, *supra* note 11, ("The fact that WCPSA imposes heightened privacy protection for a customer's call loca-

states that "[a] customer shall not be considered to have approved the use or disclosure of or access to" CSLI.[135] This indicates Congress did not intend CSLI to be treated as normal business records and should not be governed by that line of Supreme Court precedent, because that analysis "depends on assuming customers have consented to disclosure."[136] The federal statutory protection in the WCPSA provides much greater instruction for how to treat CSLI than ECPA, which was passed well before legislators conceived of the capabilities of modern cell phone tracking.

4. Normative Considerations Demand a Warrant Requirement for CSLI

Based on a normative inquiry, it is clear that the second prong of the *Katz* test is satisfied, and society is entitled to a legitimate expectation of privacy in CSLI. The pervasiveness of cell phones in society, combined with the fact that most Americans keep their cell phone on their person at all times, allows cell service providers to store records of the location of "almost every American at almost every time of day and night."[137] When the government obtains CSLI, it can retrace the steps of a cell phone user's physical movements and ultimately create a map of his life, learning "the many things we reveal about ourselves through our physical presence."[138] Courts and legislatures on both the federal and state level have indicated that location information is sensitive, personal, and subject to special protection.

---

tion information is highly relevant, especially given that the topic of wireless phone location is specifically mentioned in only one other federal statute, CALEA, which forbids its acquisition by law enforcement under the very relaxed standard for pen registers.").

135. 47 U.S.C. § 222(f)(1) (2008).

136. *Fourth Amendment*, *supra* note 91, at 1227; *see In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 841–42 (noting that the WCPSA establishes that cell-site data is "not a proprietary business record subject to unfettered corporate control").

137. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011); *see also Eleventh Circuit Opinion*, *supra* note 28 (holding that "one's cell phone, unlike an automobile, can accompany its owner anywhere" and exposure of a cell phone user's location data "can convert what would otherwise be a private event into a public one.").

138. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d at 115; *see also Eleventh Circuit Opinion*, *supra* note 28, at 1216 (explaining that "there is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (discussing how the government can use CSLI to discern whether the cell phone user is a "weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, [or] an associate of particular individuals or political groups."); United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (expressing doubt that people "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on."); State v. Earls, 70 A.3d 630, 642 (N.J. 2013) (finding a cell user's privacy expectation in their location data to be reasonable because such information can "provide an intimate picture of one's daily life" by revealing "not just where people go . . . but also the people and groups they choose to affiliate with and when they actually do so.").

The Fourth Amendment cannot be read to "impose" on society "the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society."[139] The Fourth Amendment protects reasonable expectations of privacy, and a normative inquiry proves that CSLI is exactly the type of private information that must be zealously guarded from government exploitation.

The solution cannot be to rely on shortcuts such as the third-party doctrine or the public/private distinction, as these mechanisms are created by Supreme Court cases from the 1970s and 80s. Those cases "addressed primitive ancestors of the electronic communications technologies in use today."[140] Any effort to distinguish historical CSLI from other types of protected information depends on a fundamental misunderstanding of the Fourth Amendment, as it requires the assumption that the private nature of information can somehow be meaningless to the constitutional analysis.

IV. The Third-Party Doctrine Does Not Apply to CSLI

When an individual discloses information to a third party, the third-party doctrine states the individual has given up his Fourth Amendment rights regarding the revealed information.[141] The doctrine, articulated by the Supreme Court in *United States v. Miller*, stems from the *Katz* test and draws on the idea that an individual no longer has a reasonable expectation of privacy in information revealed to third parties.[142] This doctrine has been criticized by Fourth Amendment scholars as fundamentally wrong and misguided.[143] Criticism aside, such a doctrine is inapt in the context of modern cell phone technology, for three main reasons: (1) CSLI is not an ordinary business record, (2) CSLI is analogous to "content" information, and (3) CSLI is not voluntarily conveyed by the cell phone user to a third party. The privacy concerns raised by government access to CSLI should not be

139. *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 596 (E.D.N.Y. 2010), *rev'd* (Nov. 29, 2010).

140. Freiwald, *supra* note 5, at 682.

141. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 (2009).

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

143. *See, e.g.*, Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, §§ 2.7(b)–(c) (4th ed. 2004) (describing the Supreme Court's decisions applying the third-party doctrine as making a "mockery of the Fourth Amendment"); Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment, 151–64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211 (2006) (arguing that the major third-party doctrine cases were wrongly decided on several grounds); Freiwald, *supra* note 7; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 Yale L.J. 1086, 1092 (2006) (arguing that the Supreme Court should overrule the third-party doctrine).

discarded by resort to the third-party doctrine, because "the digital age" has dramatically altered the "societal landscape" since the 1970s.[144]

A. *CSLI is Not an Ordinary Business Record*

United States v. Miller and *Smith v. Maryland* are the two Supreme Court cases which apply the third-party doctrine, and they establish that bank statements and pen register records are accessible without a warrant because they are obtained by a third party in their ordinary course of business.[145] Both of these cases were decided in the late 1970's, an era that predates cell phones.[146] This fact alone is enough to suggest that these cases should not control courts' treatment of CSLI, as the data at issue is fundamentally different.[147] CSLI records are more analogous to the records of a tracking device than ordinary business records, as the information is a collection of signal transmissions which the cell phone generates automatically just by operating.[148]

In the case of both *Miller* and *Smith*, the customer was provided with receipts and monthly statements of their transactions with the third party, which organized the information and presented it to the customer for review. There is no analogous receipt or monthly statement presented to a cell phone user regarding his *location* information. Indeed, CSLI is "neither tangible nor visible to a cell phone user."[149] As a practical matter, records of CSLI appear radically different than any kind of business record or "bill that a

144. Commonwealth v. Augustine 4 N.E.3d 846, 859 (Mass. 2014).

145. *Miller*, 425 U.S. at 442–43 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 746–747 (1979). Courts treating historical data differently than real-time data have generally relied on *Miller* and *Smith* without offering any explanation as to why it should be treated differently. *See, e.g.*, United States v. Benford, No.2:09 CR 89, 2010 WL 1266507, at *2–3 (N.D. Ind. Mar. 26, 2010)(holding that by "having no Seventh Circuit precedent on the issue, this court is persuaded by the well-reasoned decision of the Suarez-Blanca court that the logic of the Supreme Court in Smith and Miller should be extended to cell-site data."); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (relying on Smith and Miller in determining that "historical cell site information is akin to other business records maintained in the course of business"); *see also In re* United States for an Order Authorizing the Installation and Use of a Pen Register & Trap & Trace Device, 622 F. Supp. 2d 411, 418 n.8 (S.D. Tex. 2007) (holding that "this court concludes that a request for historical cell-site data when the phone is idle does not raise the same concerns as might a request for real-time cell-site data when the phone is idle.")

146. *See Augustine,* 4 N.E.3d 846, 857 (Mass. 2014) ("The [third-party] doctrine has its roots in a pair of United States Supreme Court cases that predate cellular telephones.")

147. See section III-B-iii for discussion on how federal statute, WCPSA, indicates that CSLI should not be considered under the third-party doctrine.

148. *See Third Circuit Opinion*, *supra* note 8, at 312. ("If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject.")

149. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011).

customer would actually see."[150] Unlike bank statements or pen register records, "CSLI is not subject to general understanding any more than the operation of a satellite television signal," and just to interpret the data, one must have "an understanding of radio frequency engineering."[151] In the Third Circuit litigation, the exemplar provided by the government "had none of the trappings of a communication with a customer, such as the subscriber's name, account number, or address," but rather appeared to be a report drawn from a database of raw location data.[152] In another case, the provider actually digitally transmitted the CSLI stored in their system to a government-maintained computer, and then the government had to use a software program to translate the data into a usable spreadsheet.[153] This transfer of raw data is certainly not analogous to ordinary business records provided by a bank or pen register, which are comprehensible without any interpretation or translation. This raw data is unfiltered, unorganized, and only translated by the government after it has obtained the information.

Miller reasoned that bank records are not "confidential communications," rather they are "negotiable instruments to be used in commercial transactions."[154] Similarly, *Smith* reasoned that pen registers are "routinely used" by phone companies to check billing operations, detect fraud, and prevent violations of law.[155] In contrast, service providers' retention of CSLI does not "generally serve any business purpose for the customer or for the provider in serving the customer," and such information is retained "principally, if not exclusively, in response to Government directive."[156] CSLI is not stored for commercial use, it is stored to provide law enforcement agents

150. Freiwald, *supra* note 5, at 734; *see In re* Application of U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) (explaining how the provider digitally transmitted stored cell site data to the government, which had to then "use a software program to translate that data into a usable spreadsheet"); *see also* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("Miller involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue [in a stored email case]" (quoting Miller, 425 U.S. at 443)).

151. En Banc Brief of the Appellant Quartavious Davis at 30, United States v. Davis, 573 Fed. App'x. 925 (11th Cir. 2014) (No. 12-12928), 2014 WL 7232613, at *30.

152. Freiwald, *supra* note 5, at 717 (citing Exemplar, Brief for the United States, Exhibit C, Document 11-4, *Third Circuit Opinion supra* note 8, (No. 08-4227), 2009 WL 3866618).

153. *In re* Application of U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d at 438.

154. United States v. Miller, 425 U.S. 435, 442 (1976).

155. Smith v. Maryland, 442 U.S. 735, 742 (1979) (citing United States v. New York Tel. Co., 434 U.S. 159, 174–175 (1977)).

156. *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 615 (W.D. Pa. 2008) *vacated*, *Third Circuit Opinion*, *supra* note 8; *see supra* Part II-C discussing AT&T practices; *see also* Freiwald, *supra* note 5, at 718 (stating that service providers store location data "in anticipation of law enforcement requests.").

with tracking information, and therefore it cannot be treated as an ordinary business record.

B. *CSLI is Analogous to Content*

Since Katz, the Supreme Court has incorporated "an examination of intrusiveness into its assessment of objective reasonableness."[157] In both *Miller* and *Smith*, the Court emphasized that the nature of the information at issue is a critical part of the Fourth Amendment analysis.[158] In *Smith*, the Court distinguished between content and non-content information, and the limited amount of data a pen register could record was highly relevant to the Court's determination.[159] The content/non-content distinction was included in the SCA, which protects content by a warrant requirement, and leaves non-content unprotected.[160] As noted above, this statute was passed in 1986, "well before the explosion of new communications technologies"[161] and it does not consider the implications of such a distinction for CSLI.[162] As *Smith* illustrates, the determination of whether information is content or non-content requires consideration of the nature of the information. The distinction must be understood in light of evolving technology, and the fact that modern cell phone technology is not hindered by the "limited capabilities" of a pen register[163] proves that it is "questionable and far from clearly established" whether *Smith* can justify applying the third-party doctrine to CSLI.[164]

While *Smith* offers guidance by encouraging an assessment of the nature of the information, it is commonly misapplied by courts to classify CSLI as a third-party business record, unprotected by the Fourth Amendment.[165] The

157. Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 430 (2007).

158. *See* United States v. Miller, 425 U.S. 435, 442 (1976) ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."); Smith v. Maryland, 442 U.S. 735, 741 (1979) ("[I]t is important to begin by specifying precisely the nature of the state activity that is challenged.").

159. *Smith*, 442 U.S. at 741.

160. *See supra* Part I-A on the Stored Communications Act.

161. Freiwald, *supra* note 5, at 740.

162. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1277 (2004) ("[The] ECPA was amended a number of times, although these amendments made relatively minor changes to the structure of ECPA."); *see also* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 814 (2003) ("Although ECPA has been amended many times since 1986, the 1986 Act set the basic framework of Internet surveillance law: all subsequent changes have merely nibbled around the edges of the law.").

163. *Smith*, 442 U.S. at 741.

164. Rehberg v. Paulk, 611 F.3d 828, 847 (11th Cir. 2010).

165. *See Fourth Amendment supra* note 91, at 1220, 1224 (discussing how the Fifth Circuit determined that cell site data are business records governed by *Smith* and used that finding as dispositive of the Fourth Amendment question, and stating that the Fifth Circuit

pen register record in *Smith* showed a mere three days' worth of numbers dialed out from a landline telephone, which was installed at an address provided to the phone company when service was requested. Therefore, *Smith*'s holding has little relevance in the context of CSLI. A cell phone is undeniably distinguishable from a landline phone in a "fixed location such as a residence," because "a cell phone accompanies its user throughout the day" making location information obtainable at any given point.[166] In the words of one Magistrate Judge, "Two months' worth of hourly tracking data will inevitably reveal a rich slice of the [cell phone] user's life, activities, and associations [. . .] If the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera."[167]

Fortunately, an increasing number of courts have recognized that reasonable expectations of privacy are not extinguished just because a third party stores the information.[168] For example, the Eleventh Circuit reasoned that the Fourth Amendment protection covering content should also cover "the transmission of [content] itself when it reveals information about the personal source of the transmission, specifically his location."[169] The court recognized that CSLI is "private in nature" and analogized it to communications data, as "even one point of [CSLI] can be within a reasonable expectation of privacy."[170] The Eleventh Circuit analyzed the content/non-content distinction with an eye toward the sensitive nature of CSLI, concluding that such data requires the same protection that the SCA grants to "content" information. Similarly, a district court in New York recognized "there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private."[171] These opinions reflect the growing view that a normative inquiry is necessary to a proper Fourth Amendment analysis, and because government access to CSLI is as

---

"unwisely declined to apply a normative analysis asking whether location data *should* be protected by the Fourth Amendment") (citing *Fifth Circuit Opinion*, *supra* note 11); *see also id.* (stating that the Fifth Circuit "unwisely declined to apply a normative analysis asking whether location data *should* be protected by the Fourth Amendment") (emphasis added).

166. *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 836 n.67 (S.D. Tex. 2010), *vacated*, *Fifth Circuit Opinion*, *supra* note 11.

167. *Id.* at 846.

168. *See* section III-B-ii on courts adopting a normative approach in context of CSLI. *See also* Ex Parte Jackson, 96 U.S. 727, 733 (1877) (explaining that letters do not lose Fourth Amendment protection despite being deposited with the post office and handled by numerous other people); United States v. Warshak, 631 F.3d 266, 286–87 (6th Cir. 2011) (emphasizing that the fact that a third party may access or even chooses to access information or data fails "to extinguish a reasonable expectation of privacy.").

169. *Eleventh Circuit Opinion*, *supra* note 28, at 1213.

170. *Id.* at 1216.

171. *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125–126 (E.D.N.Y. 2011).

intrusive as government access to content information, it should be granted equal protection.

C. *Cell Phone Users Do Not Voluntarily Convey Their Location Information*

Application of the third-party doctrine is further inappropriate in the context of CSLI because the cell phone user does not "voluntarily convey" their location information when making or receiving a call, let alone simply by turning on their cell phones. *Miller* and *Smith* both emphasize that the defendant "voluntarily conveyed" the information to a third party, thereby waiving any reasonable expectation of privacy. The act of using a cell phone, or merely having it turned on, generates location data as a by-product, and such an act cannot be regarded as an indication that an individual has no interest in maintaining their privacy.[172]

The Court's holding in *Miller* relied heavily on its finding that "all of the documents obtained [by the government], 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."[173] The *Smith* Court similarly relied on the notion that when dialing a phone number, the caller "voluntarily conveys numerical information to the telephone company."[174] It is worth noting that Justice Brennan questioned the reasoning in *Miller*, recognizing that "for all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[175] Justice Brennan's point would apply with greater force to CSLI as cell phone use in modern society permeates daily life to such an extent it would hardly be reasonable to expect individuals seeking privacy to simply not own a cell phone.[176] Even if we assume, however, that the reasoning in *Miller* is sound, *Miller* and *Smith* do not apply to CSLI because a cell phone user's conduct

172. *See* En Banc Brief of the Appellant Quartavious Davis at 30, United States v. Davis, 573 F. App'x 925 (11th Cir. 2014) (No. 12-12928), 2014 WL 6526854 at *15 ("the simple act of using, or even carrying, a cell phone, which has the by-product of generating location data, does not indicate a disinterest in maintaining privacy.").

173. United States v. Miller, 425 U.S. 435, 442 (1976).

174. Smith v. Maryland, 442 U.S. 735, 744 (1979).

175. *Miller*, 425 U.S. at 451 (1976) (Brennan, J., dissenting).

176. *See ECPA (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 48 (2013) (testimony of Professor Matt Blaze) ("There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans, transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us.")

is "materially different from the active, deliberate choices made to disclose information in *Smith* and *Miller*."[177] CSLI is automatically transmitted "entirely independent of the [cell phone] user's input, control, or knowledge."[178] When a cell phone user makes a call, he only knowingly conveys the number dialed, and there is no indication that his location information is being stored.[179] Not to mention the cell phone user "hasn't voluntarily exposed anything at all" when he receives a call,[180] or when he merely turns on his phone, yet such actions generate CSLI that the government can access without a warrant.[181] Cell phone users can hardly be expected to know what location data their providers collect, as they are never shown any statement showing that it is stored.[182]

In the Eleventh Circuit litigation, even the prosecutor, in his closing argument, told the jury that "obviously" the defendants "probably had no idea that by bringing their cell phones with them to these robberies, they were allowing [their service provider] and now all of [the jurors] to follow their movements on the days and at the times of the robberies."[183] It is truly "fiction" that the vast majority of the American population, by choosing to carry cell phones in a world that practically demands it, also consents to warrantless government access to their location information.[184]

The government has often responded to these arguments by referencing service contracts and the fact that they typically warn cell phone customers that they collect location-relation information and may disclose such data to law-enforcement agencies.[185] Even disregarding the argument that a waiver

177. En Banc Brief of the Appellant Quartavious Davis at 30, *Davis*, 573 F.App'x 925 (11th Cir. Nov. 15, 2014) (No. 12-12928), 2014 WL 6526854 at *15.

178. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005); see *Third Circuit Opinion*, *supra* note 8 at 317–18 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."); *see also* State v. Earls, 70 A.3d 630, 641 (N.J. 2013) (stating the transmission of CSLI doesn't involve a "voluntary disclosure in a typical sense").

179. *Third Circuit Opinion*, *supra* note 8, at 317–18.

180. *Id.*

181. See section II-A discussing the technology behind CSLI.

182. *See Third Circuit Opinion*, *supra* note 8, at 317–18 ("[I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information); *see also Earls*, 70 A.3d at 643 ("Although individuals may be generally aware that their phones can be tracked, most people do not realize the extent of modern tracking capabilities and reasonably do not expect law enforcement to convert their phones into precise, possibly continuous tracking tools.").

183. *Eleventh Circuit Opinion*, *supra* note 28, at 1217 (alteration in original).

184. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D. N.Y. 2011); *see also* Tracey v. State, 152 So.3d 504, 523 (Fla. 2014), *reh'g denied* (Dec. 8, 2014).

185. *See Fifth Circuit Opinion*, *supra* note 11, at 613; *see also In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d at 121 (concluding that any "expectation of privacy in cell-site-location records, if one exists, must be anchored in something more permanent" than the "doubtful proposition" that cell phone users

of rights should not be based on a massive service contract, the Court in *Smith* addressed this argument when it stated that individuals cannot be "conditioned" as to their Fourth Amendment rights.[186] There may be circumstances in which the legal interest in protecting information from government intrusion "trumps any actual belief that it will remain private."[187] As a Federal Magistrate Judge in Texas noted, "the tech-savvy user may now understand that there is a risk that the provider can calculate and record his location and movements very precisely" but the "bare possibility of disclosure by a third party cannot by itself dispel all expectation of privacy." Such an articulation, the Judge noted, would mean that nothing would be left of *Katz*, because in 1967 it was possible for a phone company to wiretap and disclose a private conversation in a public phone booth, and that possibility did not eliminate the phone booth user's reasonable expectation of privacy in that conversation.[188]

In the words of Justice Marshall, "it is idle to speak of assuming risks in contexts where, as a practical matter, individuals have no realistic alternative."[189] People today are required to share information about themselves with third parties on a daily basis merely to complete "mundane" tasks.[190] Indeed, cell phones are "increasingly viewed as necessary to social interactions as well as the conduct of business."[191] As Justice Sotomayor recognized, *Smith's* basic "premise that an individual has no reasonable

---

are currently "unaware of the capacities of cellular technology," since "[p]ublic ignorance as to the existence of cell-site-location records. . . cannot long be maintained"); En Banc Brief for the United States of America at *24, United States v. Davis, 754 F.3d 1205 (11th Cir.) *vacated*, 573 F. App'x 925 (11th Cir. 2014) (No. 12-12928-UU), 2014 WL 7232613 at *13 ("Ignorance of undisputed and readily ascertainable facts is both ephemeral and undeserving of constitutional protection.").

186. See discussion around FN 100–101 for *Smith* statement that individuals' Fourth Amendment rights cannot be conditioned by government intrusion.

187. *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F.Supp.2d at 124.

188. *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010) *vacated*, *Fifth Circuit Opinion*, *supra* note 11 ("[I]t is possible that a carrier may open and inspect a letter or sealed package, but that risk alone does not eliminate the legitimate expectation of privacy in such effects.").

189. Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

190. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.").

191. Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014); *see ECPA (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 48 (2013) (testimony of Professor Matt Blaze) ("There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans, transforming the way we communicate with one another, do business, and obtain and manage the increasing volume

expectation of privacy in information voluntarily disclosed to third parties" is "ill-suited to the digital age" and should be reconsidered.[192] Courts should, "rather than simply characteriz[ing] the information as a third-party record and consider[ing] the inquiry finished,"[193] go a step further and analyze whether there is a reasonable expectation of privacy based on the much more intrusive, personal information revealed in CSLI.

V. The Mosaic Theory Swallows the Public/Private Distinction

The Third Circuit, ruling before the Supreme Court issued its opinion in *United States v. Jones*, incorporated two Supreme Court cases from the 1980s into its analysis, namely *United States v. Knotts*[194] and *United States v. Karo*.[195] The Third Circuit read *Knotts* as establishing a public/private distinction for understanding Fourth Amendment protections, and read the two cases together as holding that privacy interests protected by the Fourth Amendment are "confined to the interior of the home."[196] The Third Circuit failed to recognize that "outside-the-home" monitoring could also implicate Fourth Amendment rights.[197] The technological constraints of beeper surveillance in *Knotts* and the limited amount of information that can be learned about a person through beepers were critical to the Court's holding.[198] The *Knotts* Court specifically reserved the question of whether a case involving "twenty-four-hour surveillance" would require a warrant, stating "if such dragnet-type law enforcement practices" should occur, "different constitutional principles may be applicable."[199] This foreshadowed that a strict inside the home/outside the home distinction would not be dispositive in all contexts.[200]

---

of information that is available to us."), available at http://fas.org/irp/congress/2013_hr/ecpa2.pdf.

192. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

193. *See* Freiwald, *supra* note 7, at 36–49 (criticizing the tendency of courts to rely on analytic shortcuts like a "third-party" rule and a "content/non-contents" distinction rather than analyzing reasonable expectations of privacy

194. United States v. Knotts, 460 U.S. 276 (1983) (holding that people lack Fourth Amendment protection of their location information when they are in public on "open roads").

195. United States v. Karo, 468 U.S. 705 (1984) (holding that government monitoring violated the Fourth Amendment because the beeper they used could determine whether a particular article or person was in an individual's home at a particular time).

196. *Third Circuit Opinion*, *supra* note 8, 312–13.

197. Freiwald, *supra* note 5, at 685.

198. *Knotts*, 460 U.S. at 277, 281.

199. *Id.* at 281.

200. *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 117 (E.D.N.Y. 2011) (noting that *Karo* and *Knotts* when read together show that the location and potentially quantity of information obtained by the Government are important to a Fourth Amendment analysis).

The public/private distinction should be reconsidered in light of the D.C. Circuit's opinion in *United States v. Maynard* and the Supreme Court Justices' concurrences in *United States v. Jones*, because these are written with the sensitive nature of location information and the evolved technology of cell phones in mind. Though both cases address GPS tracking, the evolution of cell tower technology and the personal character of modern cell phones make CSLI functionally equivalent to GPS data—if not more revealing.[201] These cases establish what is referred to as the "mosaic theory" approach to the Fourth Amendment. The mosaic theory requires courts to view government conduct as a "collective whole rather than in isolated steps."[202] Rooted in the concept of aggregation, it considers "whether a series of acts that are not searches in isolation amount to a search when considered as a group."[203]

The mosaic theory appears to provide a useful framework for considering CSLI, based on the amount of information collected by service providers and the scope of government requests; however, this theory will not always adequately protect cell phone users from government intrusion on their Fourth Amendment rights. Even a single point of CSLI can intrude on a legitimate expectation of privacy, and for that reason any line-drawing exercise under a mosaic theory approach would be misguided.

A. *Development of the Mosaic Theory*

The Mosaic Theory originally took form in the D.C. Circuit's decision in *United States v. Maynard*, where the court found that the public/private distinction in *Knotts* and *Karo* did not determine whether the use of prolonged GPS tracking data violates the Fourth Amendment.[204] The *Maynard* court rejected the government's argument that the defendant had no reasonable expectation of privacy in his location information because he was driving in public, explaining that "[t]he whole of one's movements over the course of a month. . . reveals far more than the individual movements it comprises" and "[t]he difference is not one of degree but of kind."[205] The *Maynard* court effectively rejected a limited reading of the Supreme Court's 1980s precedent, and embraced the notion that prolonged surveillance, even in a public space, can violate legitimate expectations of privacy.

In *United States v. Jones*, the Supreme Court reviewed and affirmed the *Maynard* decision, but the justices stated different reasons as to why. Justice Scalia wrote for the majority, deciding the case based on a trespass theory of the Fourth Amendment and thereby never addressing the reasoning in *May-*

201. See section II-A and II-D for discussion on the precision of cell site location data.
202. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).
203. *Id.*
204. *See* United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir.2010).
205. *Id.* at 561–62.

nard.[206] Five justices, through concurring opinions, expressed that an individual has a reasonable expectation of privacy in location information with respect to government monitoring over a prolonged period, suggesting they embrace the mosaic theory approach to the Fourth Amendment.[207] Justice Alito, writing on behalf of three other justices, considered whether the entirety of the monitoring over twenty-eight days exceeded societal expectations, and concluded that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[208] While Justice Sotomayor joined the majority opinion, she wrote separately to express that the use of the "unique attributes of GPS monitoring" constituted a search independent of its installation on the car, because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[209] Justice Sotomayor stated that she would consider these unique attributes when deciding whether people reasonably expect that the sum of their public movements will be stored and used by the Government to track their location.[210] These concurring opinions show five Supreme Court justices suggesting that prolonged government surveillance of an individual, even while they are in public, can implicate Fourth Amendment concerns based on the amount of personal information such a collection of data could reveal.

B. *The Mosaic Theory Fails to Adequately Protect CSLI*

Several lower courts have embraced the mosaic theory and applied its logic to historical CSLI, finding it must be protected by the Fourth Amendment warrant requirement.[211] The application of the mosaic theory to historical CSLI, however, presents a line drawing problem and would not adequately protect an individual's expectation of privacy. This is illustrated in *United States v. Skinner*, where the Sixth Circuit held that three days' worth of government monitoring of a defendant's phone GPS data was the type of "relatively short-term monitoring" which did not violate any reason-

206. United States v. Jones, 132 S. Ct. 945, 951–54 (2012).
207. *Id.* at 963–64 (Alito, J., concurring); *id.* at 956 (Sotomayor, J., concurring).
208. *Id.* at 964 (Alito, J., concurring).
209. *Id.* at 955 (Sotomayor, J., concurring).
210. *Id.* at 956 (Sotomayor, J., concurring).
211. *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011); *see also In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010) (following *Maynard* and denying warrantless requests for location data as a violation of the Fourth Amendment) *vacated*, *Fifth Circuit Opinion*, *supra* note 11; *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 581-85 (E.D.N.Y. 2010) (applying the *Maynard* approach to location data obtained from cell phones), *reversed* (Nov. 29, 2010).

able expectation of privacy.[212] The court failed to articulate why three days' worth of monitoring did not violate the Fourth Amendment, and it made things even less clear for lower courts by noting that situations may arise where the government so comprehensively tracks an individual that "the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes."[213] Subsequently, a district court in Michigan found that "when the government requests authorization to engage in long-term, real-time tracking of an individual's movements via his or her cell phone, the situation reaches past the law set forth in *Skinner*, and Fourth Amendment concerns are implicated."[214] These cases illustrate that *Maynard* and the *Jones* concurrences do not draw a precise line between short-term and long-term monitoring. They do offer some guidance, in showing that the surveillance was "long-term" at some point before four weeks, but this leaves lower courts hesitant to draw a precise line as to what constitutes unreasonable surveillance under the Fourth Amendment.

In the context of CSLI, such a line drawing exercise would be ineffective, because even one point of such information may invade a legitimate expectation of privacy.[215] One point of location data could reveal an individual in a private setting, such as in their home, or "near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute," and there is no way to know ahead of time what the CSLI could reveal.[216] Therefore, it is necessary to require law enforcement agents to obtain a warrant before gaining access to CSLI, because whether the request is limited to a single data point or three months' worth of data, it implicates the same privacy concerns for Fourth Amendment purposes.

---

212. United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

213. *Id.* at 780 (citing *Jones*, 132 S. Ct. at 964 (2012) (Alito, J., concurring)).

214. United States v. Powell, 943 F. Supp. 2d 759, 776–77 (E.D. Mich. 2013).

215. *See Eleventh Circuit Opinion*, *supra* note 28, at 1216 ("cell site data is more like communications data than it is like GPS information. That is, it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private."); *see also id.*, 943 F. Supp. at 775 ("If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant.")

216. *See Eleventh Circuit Opinion*, *supra* note 28, at 1216; *see also In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 827, 837 (S.D. Tex. 2010) *vacated*, *Fifth Circuit Opinion*, *supra* note 11 ("Like the thermal imaging devices in *Kyllo*, the cellular location technology in use or development today crosses the firm but also bright Fourth Amendment line that the Supreme Court has drawn at the entrance to the house.") (internal quotation omitted).

VI. A Judicial Solution Is Needed to Protect Cell Phone Users' Legitimate Expectation of Privacy in CSLI

Ultimately, the only way to address CSLI is by conducting a normative analysis. Courts should go further than the third-party doctrine or mosaic theory in their Fourth Amendment analysis; they "should consider asking not only whether cell phone users do in fact expect privacy in their location data, but also whether they should."[217] In the words of Justice Sotomayor, courts must ask whether the government intrusion "alter[s] the relationship between citizen and government in a way that is inimical to democratic society."[218]

The solution to this issue is for courts to require a warrant for all types of CSLI. This data is analogous to tracking information and the sensitive nature of such information requires Fourth Amendment protection. Allowing the government to obtain such information without requiring a showing of probable cause has led them to exploit this information and request extensive amounts of data about innocent parties.[219] A warrant requirement would not only guard against such extensive requests,[220] but it would also introduce procedural safeguards such as "the need to provide notice to the target, after the fact judicial review, and meaningful remedies," all of which should make a "significant difference."[221] The "intrusiveness of the method and its susceptibility to abuse" support the conclusion that a probable cause standard is necessary to protect cell phone users' Fourth Amendment rights.[222]

There is a recognized societal interest in ensuring "that guilt shall not escape or innocence suffer."[223] However, the desire to bring the guilty to justice does not outweigh the desire to protect innocent individuals from suffering intrusions on their Fourth Amendment rights. In the words of Sir William Blackstone: "The law holds that it is better that ten guilty persons escape than that one innocent suffer."[224] Adding a warrant requirement protects both interests, as it certainly does not make it impossible for the government to access such data, it simply requires them to show probable cause.

---

217. *Fourth Amendment*, *supra* note 91, at 1220–21.

218. *Jones*, 132 S. Ct. at 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J. concurring)).

219. See section II-B discussing the nature of government requests.

220. Filling out the application for a warrant forces law enforcement agents to justify the request to the courts and also to themselves. Writing an affidavit as part of the application for a warrant requires the agent to make his request under oath, and as a practical matter, the time and effort that would go into writing the affidavit for a warrant would limit the amount of people for whom law enforcement agents could request their information. *See* Fed. R. Crim. P. 41(d).

221. *See* Freiwald, *supra* note 5, at 681, 749.

222. *Id.*

223. United States v. Nixon, 418 U.S. 683, 708–09 (1974) (quoting Berger v. United States, 295 U.S. 78, 88 (1935)).

224. 4 William Blackstone, Commentaries *358.

As the Supreme Court stated, "[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."[225]

As shown by the *Jones* concurrences, it is likely that at least five of the Supreme Court Justices would be on board with a warrant requirement for historical CSLI.[226] Justice Alito's concurrence, joined by Justices Ginsburg, Breyer, and Kagan, emphasized the sensitive nature of location information and specially referred to cell phones as the most significant emerging technology shaping "the average person's expectations about the privacy of his or her daily movements" because of their ability to track and record cell phone user's physical locations.[227] This suggests these four justices are wary of the privacy implications of cell phone technology, and they would vote to protect society's legitimate expectation of privacy in CSLI. Justice Sotomayor also emphasized that location information is sensitive information that should be protected based on normative considerations, regardless of "societal expectations."[228] She also stated that entrusting to the government a surveillance technique that is "so amenable to misuse" is inappropriate and should be subject to "oversight from a coordinate branch."[229] This shows Justice Sotomayor would protect historical CSLI with a warrant requirement based on the nature of the information. Even Justice Scalia, writing for the majority, showed he would follow the "reasonable expectation of privacy test established in *Katz*" if he were to consider "[s]ituations involving merely the transmission of electronic signals without trespass," and suggested such situations might be "an unconstitutional invasion of privacy."[230] This suggests even more support on the Supreme Court for a finding that Fourth Amendment protections apply to historical CSLI.

There is certainly room for Congress to resolve this issue; however, courts cannot wait for a legislative solution to protect the millions of Americans whose privacy interests are at stake.[231] As Justice Alito recognized, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" because "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[232] However, Justice Alito also stated that because "Congress and most States have not

225. United States v. Karo, 468 U.S. 705, 718 (1984).
226. See section III-B-i discussing Supreme Court support for a normative inquiry.
227. United States v. Jones, 132 S. Ct. 945, 962–63 (2012) (Alito, J., concurring).
228. *Id*. at 956 (2012) (Sotomayor, J., concurring).
229. *Id.* at 957 (Sotomayor, J., concurring).
230. *Id.* at 953–54 (Sotomayor, J., concurring).
231. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1701, 1734 (2004) ("Even with foresight, the law is bound to be lagging behind technological developments, especially given the profound specificity and detail of the current statutory regime.").
232. *Jones* 132 S. Ct. at 964 (2012) (Alito, J., concurring).

enacted statutes" regulating the GPS technology at stake in *Jones*, "the best that [courts] can do" is ask whether the government activity in a particular case "involved a degree of intrusion that a reasonable person would not have anticipated."[233]

Congress can resolve this issue in one of two ways. First, they can establish that stored CSLI is considered tracking information. By clarifying that this data is tracking information and not a wire communication, Congress would take historical CSLI outside the scope of the SCA and make it subject to the warrant requirement of Rule 41 of the Federal Rules of Criminal Procedure.[234] Second, Congress can enact separate statutory protections for CSLI. Congress has done this in the past in response to society's privacy concerns. For example, after *Miller*, Congress enacted the Right to Financial Privacy Act of 1978 "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[235] The House Report explained that, "while the Supreme Court found no constitutional right to privacy in financial records, it is clear that Congress may provide protection of individual rights beyond that afforded in the Constitution."[236] The increasing number of state and federal courts requiring a warrant to obtain CSLI, as well as actions of numerous state legislatures to require the same, has certainly put pressure on Congress to address the issue and resolve society's privacy concerns. Until that day comes, however, courts must be responsive to these concerns and stop the government from abusing cell phone user's constitutional rights.

Conclusion

The protections of the Fourth Amendment "must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[237] With CSLI, the government can "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of 'gradual and silent encroachment' into the very details of our lives that we as a society must be vigilant to prevent."[238] In 1967, the Supreme Court held that a person's phone conversation in a phone booth was protected by the Fourth amendment, stating that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[239] This principle cer-

233. *Id.*
234. *See* Fed. R. Crim. P. 41.
235. H.R. Rep. No. 95-1383, at 9305 (1978).
236. *Id*. at 9306.
237. United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).
238. Tracey v. State, 152 So.3d 504, 523 (Fla. 2014), *reh'g denied* (Dec. 8, 2014) (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 42 & n. 67 (D.D.C. 2013)).
239. Katz v. United States, 389 U.S. 347, 352 (1967).

tainly applies to cell phones today, and by denying Fourth Amendment protection to cell site location data, courts ignore the vital role that the cell phone has come to play in the lives of over 335 million Americans.[240]

240. *See Annual Wireless Industry Survey*, CTIA-The Wireless Association, (June 2014), http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (As of December 2013, there were 335.65 million wireless subscriber accounts in the United States, responsible for 2.62 trillion annual minutes of calls and 1.91 trillion annual text messages.).