BRIDGING THE CELLULAR DIVIDE: A SEARCH FOR CONSENSUS REGARDING LAW ENFORCEMENT ACCESS TO HISTORICAL CELL DATA

Zachary Ross†

TABLE OF CONTENTS

INTRODUCTION 1186
I. CELL PHONES AND CSLI 1189
A. *Cell Phones* 1189
B. *Understanding Law Enforcement Requests for CSLI: Drawing Distinctions* 1191
1. Collection Events and Quantity of Data 1191
2. Precision of CSLI 1192
II. THE ECPA: STATUTORY PROTECTIONS FOR HISTORICAL CSLI 1197
III. THE FOURTH AMENDMENT 1200
A. *Introduction* 1201
B. *Location Monitoring Technologies and the Fourth Amendment* 1202
C. Maynard *and* Jones*: Tracking and the Fourth Amendment in the Modern Era* 1204
IV. HISTORICAL CSLI CASES 1205
A. *Comprehensiveness: How Limited Is the Government's Request?* 1206
B. *Breadth of Requested Data: Applying Recent GPS Precedent to CSLI* 1210
C. *Towards a Firm One Month Rule: Mapping* Maynard *and* Jones *to CSLI* 1212
CONCLUSION 1215

† Head *de•novo* Editor, *Cardozo Law Review*. J.D. Candidate (May 2014), Benjamin N. Cardozo School of Law. Special thanks to the staff and board members of *Cardozo Law Review* for their hard work throughout the production of this Note.

INTRODUCTION

We live in an age where rapid technological advances are constantly reorganizing the fabric of society and, by extension, our self-perception as autonomous individuals.[1] Long relegated to fairy tales and fantasy, the idea of being able to see and communicate with any person, anywhere in the world, has become so embedded in popular consciousness that it is now thoroughly unremarkable. In urban areas, cameras in businesses and on street corners are ubiquitous and, when integrated, offer a comprehensive picture of our movement through physical space.[2] Financial institutions and cell phone companies create detailed logs of our location as it changes over time,[3] just as Internet service providers (ISPs) do for our movements through cyberspace.[4]

This dense web of digital connections and information flows that characterizes our world has in turn fundamentally altered the balance of power between people and the institutions that give structure to their lives.[5] The more individuals connect with, experience, and understand the world through the use of digital intermediaries such as computers, the Internet, and cell phones, the more control over the intimate details of daily life is ceded to the institutions that facilitate these connections.[6]

Technological change is often a double-edged sword—it enables and enriches our lives, but also allows for new means of exploitation and control.[7] As social, architectural, and market barriers protecting longstanding notions of personal space erode, individuals increasingly rely on the legal system as a defense to arbitrary invasions of privacy.[8] Paradoxically, the same forces that make the need for robust privacy

---

1 *See, e.g.*, Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

2 *See generally* LOREN SIEGEL ET AL., N.Y. CIVIL LIBERTIES UNION, WHO'S WATCHING? VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT (2006), *available at* http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf.

3 Froomkin, *supra* note 1.

4 *Id.*

5 *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

6 Slobogin, *supra* note 1.

7 *See* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 128 (2005).

8 *See generally* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998) (positing four "modalities" of regulatory function); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (discussing the interaction of these four modalities in cyberspace).

protections more compelling also make the existing legal framework outdated and inapposite.[9]

These contradictions are readily apparent in the contemporary debate over the legal restrictions on government access to cell site location information (CSLI). This data, constantly collected by cell phone service providers (CSPs) in order to manage their networks,[10] has the potential to provide a detailed map of an individual cell user's movements from place to place over extended periods of time.[11] Furthermore, the quantity and precision of location data collected by CSPs is constantly increasing, becoming more revealing, and more valuable to law enforcement in the process.[12] Despite the potential intimacy of this data and its growing relevance to criminal investigations, the legal protection afforded CSLI is hotly disputed, and at present varies greatly among (and sometimes even within) jurisdictions—with courts sometimes requiring a warrant, and sometimes allowing unfettered access upon a lesser evidentiary showing.[13] This lack of uniformity has been exacerbated by a recent Fifth Circuit ruling on government access to CSLI,[14] which generated a different rule than had previously been adopted by the Third Circuit.[15] The vastly disparate treatment of government requests for CSLI has

9 That the very notion of "privacy" has historically been a notoriously vague and nebulous concept only compounds the problem of affording it legal protection. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 478 (2006) ("Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of 'privacy' do not fare well when pitted against more concretely stated countervailing interests.").

10 For an excellent summary of the technology behind CSLI and cell networks, see Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATT'YS BULL. 16, 17 (2011), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf (discussing why historical CSLI is "reliable, accurate, and useful in criminal trials").

11 *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 838 (S.D. Tex. 2010) (stating that CSLI has the potential to "expos[e] . . . a person's movements, activities, and associations in relentless detail"), *vacated*, 724 F.3d 600 (5th Cir. 2013). CSLI data is further defined in *infra* Part I.

12 Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 120 (2012) ("Law enforcement agencies—already using location information in their investigations—are likely to increase their reliance on such information as technology improves.").

13 *Id.* at 122. This trend is likely exacerbated by the government's decision not to appeal unfavorable decisions, leading to a patchwork of lower court decisions and a dearth of binding precedent on the issue. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 682 (2011) ("[E]xecutive branch litigators have themselves strategically avoided appealing cases to preserve the prerogatives that a definitive constitutional ruling against them would eliminate.").

14 *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

15 *In re* 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).

created a chaotic system ripe for abuse,[16] and all but guaranteed Supreme Court review of the issue in the near future, as the Court itself seems to have implicitly acknowledged.[17]

This Note will examine the complex interaction between privacy, surveillance, and technology through an exploration of the contested legal terrain governing law enforcement access to *historical* CSLI—location data recorded by CSPs which reveal an individual's *past* movements.[18] In doing so, this Note will draw from the dozens of opinions that have been authored by magistrate, district, and circuit court judges on this topic since 2005. Part I will provide a brief description of the cell phone technology and CSLI, and how it is used by law enforcement. Part II will feature an overview of the relevant statutory framework governing stored electronic communications and the various conflicting interpretations of its application to CSLI. Part III will provide a basic background on Fourth Amendment jurisprudence, and an overview of recent developments as they relate to government access to historical CSLI. Part IV will synthesize a wide range of judicial opinions issued on CSLI in an attempt to mark out some areas of tentative agreement among apparently disparate approaches. This Part will argue that there is evidence of an emerging consensus among justices that more comprehensive CSLI requests should not be accessible without a warrant supported by probable cause. Furthermore, drawing upon the most recent decisions regarding the constitutionality of long-term Global Positioning System (GPS) tracking, this Note will propose that the same warrant standard should be applied to government requests for data that seek more than one month's worth of historical location information culled from cell phone networks.

---

16 *See* Michael Isikoff, *The Snitch in Your Pocket; Law Enforcement Is Tracking Americans' Cell Phones in Real Time—Without the Benefit of a Warrant*, NEWSWEEK, Mar. 1, 2010, at 40.

17 *Compare* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (noting that the majority's resolution of the case "will present particularly vexing problems" where surveillance is undertaken through solely electronic means), *with id.* at 954 (majority opinion) ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

18 This term is used to distinguish the subject matter of this Note from CSLI that is used to track a suspect's *present* movements in real time. That class of data is known as *prospective* CSLI and is often analyzed differently by courts. *See In re* U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 535 n.4 (D. Md. 2011); *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 829–30 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

I. CELL PHONES AND CSLI

A. *Cell Phones*

Cell phones have become indispensable and ever-present features of modern life.[19] Although a relatively rare and impractical luxury little more than twenty years ago, today 85% of Americans own a cell phone,[20] and the professional and personal demands of contemporary life belie the notion that most people can simply choose whether or not to carry a cell phone.[21] Meanwhile, cell phones have evolved to handle not merely calls, but also text messaging, video chat, e-mail, and Internet access—in the process becoming an increasingly instrumental conduit to the outside world.[22] Put simply, more people are using cell phones to do more things every day, and this trend is unlikely to reverse itself anytime soon.[23]

As cell phones have become more popular, more sophisticated, and more prominent in our daily lives, the demands placed on cell phone networks have grown exponentially.[24] Cell phones are able to connect users to the larger network through the use of cell towers (or "sites"), which are essentially antennas of varying size and range distributed geographically in an overlapping grid formation to provide continuous coverage.[25] In areas of higher usage, such as urban areas, the network of cell towers must be denser—more sites are needed to provide the capacity to meet increased demand placed on the network.[26]

---

19 O'Malley, *supra* note 10, at 22–23. It seems 2012 was a landmark year for the wireless industry—the number of active wireless connections surpassed the total population of the United States for the first time. *See Wireless Quick Facts*, CTIA—THE WIRELESS ASS'N (June 2012), http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

20 MAEVE DUGGAN & LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, PEW RESEARCH CTR., CELL PHONE ACTIVITIES 2012 2 (Nov. 25, 2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf.

21 Supplemental Brief of Amicus Curiae Electronic Privacy Information Center at 1, State v. Earls, 70 A.3d 630 (N.J. 2013) (No. 68,765), *available at* http://epic.org/amicus/location/earls/EPIC-Supplemental-Amicus-Brief.pdf ("Cell phones have become ubiquitous, and are an essential tool in the everyday lives of most Americans.").

22 DUGGAN & RAINIE, *supra* note 20.

23 O'Malley, *supra* note 10, at 22 ("The dramatic evolution of cell phone equipment and, more importantly, drastic price reductions for cell phones and cell phone service plans, have driven explosive growth in cell phone ownership, usage, and coverage throughout the United States and the world.").

24 *Id.*

25 *Id.* at 18–22.

26 Pell & Soghoian, *supra* note 12, at 127. As of June 2012, there were 285,561 cell sites in the United States. *Wireless Quick Facts*, *supra* note 19. When the ECPA was passed, there were only 913 cell sites in operation. *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

Alongside expansion in the customer base, the rise of smartphones[27] and the desire for faster connection speeds to enable these advanced devices (3G, 4G) have exacerbated the burden on the network, forcing improvements to its carrying capacity.[28] As a result of these trends, the number of cell towers tripled between 2000 and 2010.[29] Critically, this has led cell towers to become not only more numerous, but also smaller in service area.[30] In high traffic areas, CSPs have begun placing greater reliance on "picocell" or "femtocell" technologies,[31] which unlike conventional cell towers, have ranges of as little as forty feet.[32] These smaller sites are often responsible for dealing with capacity issues in dead-spots—small spaces such as elevators and areas of office buildings where cell reception would otherwise be weaker due to interference.[33] Femtocells are becoming an increasingly important part of wireless network infrastructure[34] and now outnumber traditional cell sites world-wide.[35]

---

27 Smartphones are characterized by large screens, high-speed data connections, advanced operating systems, and sophisticated input devices such as keyboards or touch screens. Supplemental Brief of Amicus Curiae Electronic Privacy Information Center, *supra* note 21, at 7. As of 2012, approximately 50% of U.S. subscribers owned smartphones. *Id.*

28 Pell & Soghoian, *supra* note 12, at 132–35 ("[T]he success of Apple's iPhone and other smartphones has led to a massive increase in the use of data by mobile users. . . . AT&T has seen an *8,000 percent* increase in data traffic between 2007 and 2010." (emphasis added)).

29 See *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, for an excellent review of the current state of wireless network technology as it relates to CSLI and tracking.

30 *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. 15 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) [hereinafter *June Hearings*], *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf ("[T]he size of a sector today is far smaller than it was 25 years ago because of the natural evolution of the technology.").

31 Femtocells connect directly to a customer's broadband network and provide cell service within a limited range, often no further than the subscriber's residence. Pell & Soghoian, *supra* note 12, at 132.

32 *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 833; Dimitris Mavrakis, *Do We Really Need Femto Cells?*, VISION MOBILE (Dec. 1, 2007), http://www.visionmobile.com/blog/2007/12/do-we-really-need-femto-cells.

33 *June Hearings*, *supra* note 30, at 15–16 ("[T]he latest technology has trended toward what are called variously microcells, picocells and femtocells that are designed . . . to serve a very, very specific location, such as a floor of a building or even an individual room in a building . . . or an office complex or hotel or even a private home.").

34 As one market research firm recently stated:

> Femtocell is rapidly emerging as a fundamental technology enabler in the deployment of next generation (3G/4G) wireless network infrastructure. . . . Using femtocell, a wireless operator can improve both coverage and capacity especially in an indoor area, where access would otherwise be limited or unavailable, in a highly cost effective way. This will reduce the carriers operating costs as well as capital expenditures.

Zacks Equity Research, *Femtocell—The Emerging Wave*, YAHOO! FIN. (Jan. 2, 2013, 12:43 PM), http://finance.yahoo.com/news/femtocell-emerging-wave-174356640.html.

35 *Small Cells Outnumber Traditional Mobile Base Stations According to Informa Report*, REUTERS (Oct. 31, 2012, 5:52 AM), http://www.reuters.com/article/2012/10/31/idUS125206+

B. *Understanding Law Enforcement Requests for CSLI: Drawing Distinctions*

Management of this cellular network requires CSPs to collect considerable amounts of data from cell users.[36] This data is not limited to obvious information collected for billing purposes, such as records of incoming and outgoing phone numbers, call duration, text and data usage, and the like, but also information about which cell sites an individual phone communicates with as it moves about the coverage area.[37] This Note is concerned with this latter type of data, CSLI, which can be used to fix an individual's relative location at the time it was collected.

1. Collection Events and Quantity of Data

A variety of events will trigger the collection of CSLI. A cell phone that is powered on is in constant communication with the network through the process of "registration," by which a cellular device will automatically make contact with nearby towers, without the user's input or awareness.[38] This passive registration process may take place as often as every seven seconds.[39] Locational data is also collected when a user actively connects to the network, for example, when a call is made or received, as well as during the duration of a call.[40] This "active use" data may likewise be collected when making or receiving a text message, checking e-mail, or using the Internet.[41] However, unlike passive registration CSLI, the quantity of this data is dependent on the cell user's voluntary interactions with his phone.

As is indicated by the variety of events that may trigger its collection, CSLI is not a monolithic category. In order to comprehend what is at stake when law enforcement agents request CSLI, it is first important to understand exactly what such data reveals about cell phone users. Regarding data quantity, a law enforcement request that seeks only "active use" data may provide a much less comprehensive picture

---

31-Oct-2012+BW20121031.

36 O'Malley, *supra* note 10, at 22–23.

37 *June Hearings*, *supra* note 30, at 15–16 ("This information is extraordinarily valuable for business, marketing and technical purposes. It tells them where their network needs to be improved, w[h]ere dead spots are, and how their customers use their phones."). As technology improves and data storage costs decrease, the amount of data retained is likely to increase in quantity and precision. Freiwald, *supra* note 13, at 715–16.

38 Freiwald, *supra* note 13, at 705–06.

39 *Id.* at 703.

40 *Id.* at 703–10.

41 *Id.* at 708–09; *see also* Supplemental Brief of Amicus Curiae Electronic Privacy Information Center, *supra* note 21, at 2, 11.

of a suspect's movements than a request that also includes passive registration data.[42] Further complicating the picture is the fact that CSLI varies significantly depending on the method by which it is collected. Indeed, much of the difficulty in fixing legal restrictions on government access to CSLI is the potentially tremendous variation in precision among different types of CSLI.

2. Precision of CSLI

CSLI is best understood as an umbrella term that encompasses a broad range of locational data collected by CSPs in providing service to cell phone users. The nature of this data varies greatly depending on the technology being used, both by the end user and by the CSP. On the user side, a smartphone with GPS technology will enable the CSP to collect different types of data when compared to a more basic cell phone without GPS.[43] On the service provider side, different CSPs have different protocols governing the types of data they collect.[44] Furthermore, differences in population density and geography also play a role, as a greater concentration of users, in urban areas for example, will necessitate a denser network of cell sites to compensate for the increased network demand.[45] This means that CSLI collected in urban areas is often far more precise in fixing a user's relative location than in rural areas where cell towers may be miles apart.[46] Because understanding the nature of CSLI data is critically important to understanding its appropriate legal protection, a more detailed look at the precision of different types of locational data collected is helpful.

i. GPS: Handset-Based CSLI

There are two major methods by which CSPs collect location data: handset-based (GPS) and network-based (cell site).[47] The former relies on information gathered by the cellular device itself, while the latter

---

42 *See* Freiwald, *supra* note 13, at 702 ("Each additional data point furnishes more insight into where a person has gone, and as the data becomes more finely grained, government officials can better determine when a person has arrived and departed from each place and, accordingly, how long he has remained there.").

43 *See infra* Part I.B.2.i.

44 *June Hearings*, *supra* note 30, at 27 ("While each carrier has its own data collection and retention practices, carriers typically create 'call detail records' that include the most accurate location information available to them.").

45 Freiwald, *supra* note 13, at 710.

46 *June Hearings*, *supra* note 30, at 28 ("[I]n rural areas, a sector ID might currently specify only a radius of several miles, while in a dense urban environment with microcells, it could identify a floor or even a room within a building.").

47 *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

relies on records of the phone's communication with the larger cell network to establish its relative physical location.[48] GPS technology utilizes multiple satellites to calculate a user's latitude and longitude, and is typically accurate within a ten-meter margin of error, sufficient to track a user to a particular street address.[49] This information is gathered from a GPS-enabled cell device by a CSP as the user moves throughout the CSP's coverage area.[50] There is considerable consumer interest in GPS technology, which allows users to take advantage of Google Maps and similar geolocation services.[51] However, cell phone manufacturers have also adopted GPS in order to comply with federal regulation intended to ensure accurate tracing of 911 calls.[52] As a result, GPS technology is found in almost all Internet-enabled smartphones, and also in many newer model phones[53] that lack smartphone capabilities.[54]

While GPS technology typically allows for the most accurate tracking, it does have its own inherent limitations.[55] GPS is not available on all cell phones, particularly older, less sophisticated models.[56] GPS is only accurate insofar as a clear "line of sight" can be established between a device and the satellites it communicates with, which means that GPS is less accurate in cities and often unavailable or unreliable indoors.[57] Finally, unlike other sources of CSLI, GPS technology can often be disabled by the user.[58]

---

48 *Id.* at 831–32.

49 *Id.*

50 *Id.*

51 Bonnie Cha, *Road Warriors: Smartphones with Built-In GPS*, CNET (May 14, 2010), http://reviews.cnet.com/4321-6452_7-6564140.html (GPS is "almost a must-have feature" that allows "real-time position tracking, text- and voice-guided directions, and points of interest" functionality).

52 47 C.F.R. § 20.18(h)(1)(i)–(ii), (2)(i)–(ii) (2012) (mandating that 911 calls made from cell phones be traceable within "100 meters for 67 percent of calls" and "300 meters for 90 percent of calls" for network-based (non-GPS) technologies, and "50 meters for 67 percent of calls" and "150 meters for 90 percent of calls" for handset-based (GPS) technologies).

53 For example, Verizon Wireless has included GPS-capability in every cell phone sold since 2004. Supplemental Brief of Amicus Curiae Electronic Privacy Information Center, *supra* note 21, at 5.

54 GPS tracking capability for these phones will generally be activated only when the user dials 911. *Id.* at 5–6 (noting that many modern cell phones contain GPS chips even when they cannot perform mapping or location-based functions). However in some instances, law enforcement has apparently requested access to such data. Freiwald, *supra* note 13, at 713–14.

55 Pell & Soghoian, *supra* note 12, at 129.

56 *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

57 *Id.*

58 *In re* U.S. for an Order, 411 F. Supp. 2d 678, 681 (W.D. La. 2006). Users may wish to disable GPS data because of the increased demand it puts on a cell phone's battery life. Pell & Soghoian, *supra* note 12, at 129.

ii. Network-Based CSLI

The second major source of CSLI is collected, not by technology in the cellular device itself, but by CSPs as the device communicates with various cell sites in the network.[59] There are a variety of techniques by which CSLI can be collected under this network-based approach, which may yield more or less precise locational data depending on the method used. On the most basic level, CSPs will record the cell tower used to route a particular communication.[60] As coverage areas of a single tower or cell site vary significantly, so too would the locational precision of this kind of data.[61] Knowing which tower a cellular device communicated with in North Dakota might only place a suspect within a radius of several miles. In New York City, however, this data could place a suspect within a forty-foot area.[62] If a cellular device is transferred from one cell site to another as the user moves from place to place during a call, the precision of even basic, single-tower data increases dramatically because that user could be placed in a particular area of overlapping coverage among various different cell sites.[63]

On a more advanced level, network-based CSLI may also include information about the particular "face" of the cell site with which a device communicates.[64] This data divides up the circular coverage area of a single tower into three radial "sectors"—like slices of a pie.[65] CSPs may track a user's specific sector relative to a cell site and record his movements as he goes from one sector to another.[66] Thus, even when data from only one cell tower is implicated, cell sector tracking allows for far greater accuracy than the method discussed above.[67]

Finally, all of this data may be combined with information showing the relative strength and angle of a user's cell signal as it communicates with multiple cell sites.[68] CSPs rely on a network of cell sites that provide overlapping coverage areas in order to handle shifting demand—for this reason a single cell phone may communicate with multiple sites as it is used.[69] Where signal strength data from multiple sites is collected, the user's location may be triangulated with virtually "pinpoint" accuracy.[70]

---

59 O'Malley, *supra* note 10, at 26–27.

60 *Id.*

61 Freiwald, *supra* note 13, at 710.

62 *See supra* note 46 and accompanying text.

63 Freiwald, *supra* note 13, at 710–13.

64 *Id.* at 710–11.

65 For an illustration of this process, and of the composition of cell networks in general, see O'Malley, *supra* note 10, at 19–27.

66 Freiwald, *supra* note 13, at 710–13.

67 *Id.* at 710–12.

68 *Id.* at 711–13.

69 O'Malley, *supra* note 10, at 27.

70 *In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 452 (S.D.N.Y. 2006) ("Where . . . the government obtains information

In its most sophisticated form, triangulation data approaches GPS in its ability to track a user's location.[71] However, unlike GPS, this type of data is not dependent on a particular technology within the cell phone itself (which may be turned off by the user) and does not require that the user be outside in order to communicate with satellites to establish an accurate locational fix.[72]

iii. Law Enforcement Requests: Differences in Comprehensiveness

The final major variable in cases dealing with government access to CSLI is the actual request itself, which may be relatively limited—for one or two classes of CSLI—or comprehensive, combing most or all of the data types discussed above.[73] Furthermore, requests vary dramatically in their durational scope, and may be for discrete or prolonged periods of time. For example, law enforcement may request locational information indicating only which cell tower was used to route incoming or outgoing calls over a period of a few days.[74] At the other end of the spectrum, law enforcement may make an unlimited request for any and all data collected over a period of weeks, or even months, which could include registration data continuously collected without any affirmative action taken by the user.[75]

Data received from a less limited request, as discussed above, could be used to triangulate the user's position relative to multiple cell towers with far greater accuracy than single tower information.[76] Such data would be collected not just when a customer is actively using his cellphone, but at all times the phone communicates with the network simply by virtue of being turned on.[77] Lastly, law enforcement may want to go beyond the "historical" data normally collected by CSPs and actually use an individual's cell phone to track his current movements in

from multiple towers simultaneously, it often can triangulate the caller's precise location and movements by comparing the strength, angle, and timing of the cell phone's signal measured from each of the sites.").

71 *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

72 Freiwald, *supra* note 13, at 712.

73 *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 386–87 (D. Md. 2012) (concerning applications for all historical data associated with two phone numbers, one for 14 days, the other for 213 days); *In re* U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 578–79 (E.D.N.Y. 2010) (concerning an application for all historical cell data over a fifty-eight day period), *rev'd*, Nov. 29, 2010.

74 *See, e.g.*, United States v. Skinner, No. 3:06-CR-100, 2007 WL 1556596 (E.D. Tenn. May 24, 2007) (concerning a request for cell data over a period of three days), *adhered to on reconsideration*, No. 3:07-CR-89, 2008 WL 304861 (E.D. Tenn. Jan. 31, 2008), *aff'd*, 690 F.3d 772 (6th Cir. 2012); People v. Hall, 823 N.Y.S.2d 334 (Sup. Ct. 2006) (concerning a request for historical cell data over a three-day period).

75 *See* Freiwald, *supra* note 13, at 702–09.

76 *Id.* at 710–15.

77 *Id.* at 735–40.

real time.[78] Although a detailed look at this *prospective* CSLI is beyond the scope of this Note, it is worth mentioning primarily because it is often analyzed by the courts differently than historical CSLI.[79]

As this section has illustrated, CSLI is at best a loose categorization of different kinds of data. A request to access CSLI cannot be accurately conceptualized without looking at the context in which the data was gathered and close scrutiny of the specifics of the request itself. Amidst all this uncertainty, a few points bear mention. First, as cell phones evolve, the quantity and precision of CSLI will continue to grow.[80] As people use their cell phones more often, CSPs will have more opportunities for the collection of active use data. This increased demand will necessitate more network capacity, as well as more numerous and smaller cell sites, thereby increasing the precision of CSLI.[81] In addition to GPS technology becoming more prevalent, this growth will also continue to improve the accuracy of locational data collected through network-based approaches such as triangulation.[82] The gap in accuracy between GPS and triangulation data will continue to shrink in more densely populated areas, and will likely disappear completely in many urban areas, if it has not already done so.[83] Second, from a privacy perspective, the intrusiveness of government access to CSLI varies based on the quantity and precision of the underlying data. The more data points that are available—and the more precise these data points are—the more accurate a picture law enforcement is able to paint of an individual's movements.[84]

Lastly, surveillance using CSLI provides law enforcement with significant benefits over traditional surveillance methods, in terms of both economic efficiency and practical effect.[85] As a result, law

---

78 *See Graham*, 846 F. Supp. 2d 384.

79 *See, e.g.*, *In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006).

80 Freiwald, *supra* note 13, at 715.

81 *Id.*

82 Pell & Soghoian, *supra* note 12, at 133 ("As the coverage area around each traditional cell tower shrinks, and consumers increasingly embrace femtocells in their homes and businesses, single cell site data will become far more accurate—in some cases as good as GPS . . . .").

83 *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 832–34 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

84 *Id.* at 846 ("Two months' worth of hourly tracking data will inevitably reveal a rich slice of the user's life, activities, and associations . . . .").

85 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society." (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *judgment vacated*, 132 S. Ct. 1534 (2012) (mem.)) (internal quotation marks omitted)).

enforcement requests for data have exploded in recent years,[86] and will continue to increase as improvements in precision make the data "absolutely vital" to locate suspects and uncover evidence of criminal activity.[87] This trend has already progressed to the point that some CSPs have been forced to outsource the work of processing requests to third parties in order to handle the increased volume of requests.[88] Unfortunately, as long as the legal standard governing access to CSLI remains unclear, cell phone users cannot be assured that their data receives adequate or consistent protection.

II. THE ECPA: STATUORY PROTECTIONS FOR HISTORICAL CSLI

Government access to historical CSLI is regulated by two major bodies of law: one statutory, the other constitutional. This Part provides a brief overview of the statutory restrictions on government access to CSLI contained in the Electronic Communications Privacy Act (ECPA).

Much of the difficulty in fixing appropriate legal protections to CSLI is that the statutory framework governing its access is both convoluted and outdated.[89] The Stored Communications Act (SCA),[90] the primary mechanism regulating CSLI, was passed as a subsection of the ECPA in 1986.[91] In 1994, Congress passed the Communications Assistance to Law Enforcement Act (CALEA),[92] which amended the SCA to its current manifestation.[93]

The ECPA, which has not been significantly modified since it was enacted well over two decades ago, was passed at a time when cell

---

86 Eric Lichtblau, *Cell Carriers Called on More in Surveillance*, N.Y. TIMES, July 9, 2012, at A1 (noting that requests forwarded to AT&T have tripled since 2007).

87 *Id.*

88 *Id.*

89 As James X. Dempsey of the Center for Democracy and Technology noted in a prepared statement to the House of Representatives regarding reform of the ECPA:

> While the ECPA was a forward-looking statute when enacted in 1986, technology has advanced dramatically since 1986, and the statute has been outpaced. ECPA has not undergone a significant revision since it was enacted in 1986—light years ago in internet time[.] ECPA today is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for many service providers and law enforcement agencies alike.

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. 26 (2010), *available at* http://judiciary.house.gov/hearings/printers/111th/111-98_56271.pdf.

90 18 U.S.C. §§ 2701–2711 (2012).

91 The ECPA also contains two other Titles, currently located in 18 U.S.C. §§ 2510–2522 (wiretapping), and 18 U.S.C. §§ 3121–3127 (pen register/trap and trace devices).

92 47 U.S.C. § 1001–1010 (2012).

93 *Cf.* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (showing the original version of the SCA).

phones were relatively primitive and exceedingly rare.[94] At this time, service areas were limited, and cell towers were placed miles apart to ensure maximum geographical coverage.[95] Because of the tremendous changes in the technological landscape of the country since the mid-1980s, a coalition of technology industry leaders and privacy groups have urged Congress to substantially revise the ECPA, thus far to no avail.[96]

The ECPA was passed in order to define the legal protections afforded to Americans using nascent digital communications technologies such as e-mail and wireless phone services.[97] The statute defines the means by which the government and other authorized actors, such as service providers, are permitted to access users' data, and it explicitly made unauthorized access a federal crime.[98] Title I of the ECPA concerns "wiretaps," or the interception of wire, oral, and electronic communications while in transit.[99] Title II regulates access to stored electronic communications.[100] Finally, Title III governs the use of pen register and trap and trace devices.[101] Each title proscribes a different level of legal protection to the various classes of communication based on the perceived privacy issues at stake in the information, ranging from the highest protection afforded to the contents of communications subject to a wiretap, to the lowest level of protection for data culled from pen register/trap and trace devices.[102]

Under the SCA, law enforcement "may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service" pursuant to a conventional warrant, *or*

---

94 Easily distinguishable from modern devices, cell phones circa 1986 were unwieldy and impractical; typically they took the form of car phones for the well-to-do. *See In re* U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *6 (S.D.N.Y. Jan. 13, 2009).

95 *June Hearings*, *supra* note 30.

96 *See Our Principles*, DIGITAL DUE PROCESS COALITION, http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Oct. 19, 2013). For a list of the Coalition's members, see *Who We Are*, DIGITAL DUE PROCESS COALITION, http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Oct. 19, 2013).

97 *See Our Principles*, DIGITAL DUE PROCESS COALITION, http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Oct. 19, 2013).

98 H. MARSHALL JARRETT ET AL., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

99 *Id.* at 161. The source refers to the Federal Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012), as "Title III" because it was "first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968." *Id.* at 151.

100 *Id.* at 115.

101 *Id.* at 153.

102 Pen registers and trap-and-trace devices record only the incoming and outgoing numbers dialed for a particular telephone service subscriber. *See id.*

through a court order as outlined in § 2703(d).[103] Section 2703(d) in turn indicates that a court order "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[104] The standard in § 2703(d) is an intermediate standard—lower than a warrant, which requires probable cause that the search will reveal evidence of a crime—but higher than a subpoena.[105]

Courts that have allowed government access to historical CSLI under a § 2703(d) order have offered a variety of rationales for doing so. Most decisions hold that CSLI is a customer "record" under § 2703(c), and that therefore, disclosure is mandatory upon a § 2703(d) order.[106] The Third Circuit, however, has questioned this approach.[107] Noting that the language of § 2703(d) reads that a court order "*shall* issue *only* if" the government meets the "specific and articulable facts" standard, the Third Circuit held that reviewing justices have the *discretion* to require a warrant to access historical CSLI.[108]

The logic behind this approach is essentially that § 2703(d) merely sets out a minimum standard: "[L]anguage that an order can be issued 'only if' the showing of articulable facts is made indicates that such a showing is necessary, but not automatically sufficient. If issuance of the order were not discretionary . . . the word 'only' would be superfluous."[109] The importance of the word "only" is highlighted by the fact that related statutes, such as the Pen Register Statute,[110] which allows the government to access other types of phone records, include

103 18 U.S.C. § 2703(c)(1).

104 18 U.S.C. § 2703(d).

105 S. REP. NO. 103-402, at 31 (1994) ("This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable-cause warrant. The intent of raising the standard for access to transactional data is to guard against 'fishing expeditions' by law enforcement.").

106 *In re* 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). Recently, a divided Fifth Circuit expressly rejected the Third Circuit's construction of the SCA as applied to historical CSLI, over a lengthy dissent by Judge Dennis. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 606–07 (5th Cir. 2013) (holding that the magistrate judge below lacked the authority to require a warrant for access to historical CSLI, provided the government met the minium statutory requirements of § 2703(d)); *id.* at 615–31 (Dennis, J., dissenting). The Fifth Circuit's decision thereby created a circuit split on both the constitutional and statutory issues raised by law enforcement access to historical CSLI. *Id.* at 616. Although the Fifth Circuit case somewhat diminishes the value of the Third Circuit decision as persuasive precedent regarding the appropriate construction of the SCA as applied to historical CSLI, the disagreement among circuits only enhances the importance of constitutional questions considered in the remainder of this Note.

107 *In re U.S. for an Order Directing a Provider*, 620 F.3d at 315.

108 *Id.* (quoting 18 U.S.C. § 2703(d)) (internal quotation marks omitted).

109 *Id.* at 315 (citation omitted).

110 18 U.S.C. §§ 3121–3127.

similar language without the word "only."[111] Furthermore, § 2703(c) specifically contemplates *both* a warrant and the lesser § 2703(d) standard.[112] If such judicial discretion had not been contemplated by the drafters of the statute, then by implication the choice between a warrant and a § 2703(d) order would be the sole prerogative of the government officers making the request—a somewhat absurd result given that the SCA was drafted to restrict the government's ability to access electronic information.[113] However, as the Third Circuit recognized, the distinction between requests that raise Fourth Amendment issues—and therefore require a warrant—and those that do not is not immediately clear.[114]

III. THE FOURTH AMENDMENT

The Third Circuit's approach provides a "safety valve," allowing justices to impose a warrant requirement if and when government requests for CSLI would otherwise raise Fourth Amendment issues.[115] This section will provide an overview of relevant Fourth Amendment jurisprudence as it relates to location tracking. In the surveillance context, the Fourth Amendment is generally interpreted as requiring that law enforcement activities deemed by the court to constitute a "search" take place only when supported by a warrant detailing the evidentiary basis for "probable cause"—the quantitative foundation for the belief that the search will likely uncover evidence of criminal activity.[116]

---

111 *In re U.S. for an Order Directing a Provider*, 620 F.3d at 315.

112 18 U.S.C. § 2703(c).

113 *In re U.S. for an Order Directing a Provider*, 620 F.3d at 315.

114 *Id.* at 320 (Tashima, J., concurring) (criticizing the majority's approach as "provid[ing] *no* standards for the approval or disapproval of an application for an order under § 2703(d)").

115 Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Affirmance of the District Court, *In re U.S. for an Order Directing a Provider*, 620 F.3d 304 (No. 08-4227), 2009 WL 3866619.

116 Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002). The Fourth Amendment states:

> [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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

A. *Introduction*

While early Fourth Amendment jurisprudence focused on physical trespass as the primary indicium of whether or not a search had occurred,[117] the development of modern communications and surveillance technologies has shifted the emphasis of Fourth Amendment inquiries towards the more flexible test established by the landmark Supreme Court decision in *Katz v. United States*, which focuses on whether an individual's "reasonable expectation of privacy" has been violated by law enforcement activities.[118] *Katz* rested on a distinction between two realms—areas where individuals were entitled to expect privacy and areas in which such an expectation was normatively unreasonable. Critical to this analysis was the Court's reasoning that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[119] The Court thereby set forth a dichotomy between "knowing exposure" to third parties on the one hand, and "reasonable expectation of privacy" on the other.[120] In extending Fourth

---

117 *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that wiretapping a phone line did not constitute a search absent law enforcement trespass on the defendant's property).

118 *See* Katz v. United States, 389 U.S. 347, 353–54 (1967); *id.* at 360–61 (Harlan, J., concurring). In his influential concurrence in *Katz*, Justice Harlan declared that the relevant inquiry was not whether a physical trespass had taken place, but whether the subject had "a constitutionally protected reasonable expectation of privacy" which had been breached by the government's surveillance activity. *Id.* Thus formulated, the court's duty was to ascertain "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. If both questions are answered in the affirmative, any surveillance activity violating this reasonable expectation of privacy becomes a search, which, when unsupported by a warrant, becomes "presumptively unreasonable" for constitutional purposes. *Id.*

119 *Id.* at 351 (majority opinion).

120 *Compare id.*, *with id.* at 360 (Harlan, J., concurring). In *Katz*, the Court found that when the defendant shut the door to the phone booth, his actions evidenced a subjective expectation of privacy, which the Court found to be objectively reasonable due to the vital role the public telephone played in the communications system at the time. *Id.* at 351 (majority opinion).

This distinction has in turn laid the foundation for what has become known as the "third party doctrine," which essentially holds that one cannot maintain a reasonable expectation of privacy in information voluntarily handed over to third parties. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744, (1979) ("[A] bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business." (quoting U.S. v. Miller, 425 U.S. 435, 442 (1976))). The application of the third party doctrine to historical CSLI is, like much else in this fast-changing area of law, hotly disputed. Some courts have held that it does not apply to historical CSLI, while others have reached the opposite conclusion. *Compare In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that the third party doctrine removed historical CSLI from the ambit of Fourth Amendment protection) *with In re* 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) (reaching the opposite conclusion).

Amendment analysis beyond property rights to cover intangible privacy interests, *Katz* provided the courts with a versatile tool to confront a world of new communication systems and novel surveillance techniques.[121] That said, extension of the reasonable expectation of privacy test to cover emerging surveillance technologies has also proved problematic for the Court.[122]

B. *Location Monitoring Technologies and the Fourth Amendment*

As new technologies have granted law enforcement new, vastly more efficient tools with which to track a suspect, the courts have had to consider what effect this technological development has had on Fourth Amendment analysis. The Supreme Court first considered modern location tracking technology in 1982, in *United States v. Knotts*,[123] which has since become one of the most often cited cases in the battle to define the application of the Fourth Amendment to CSLI. *Knotts* concerned law enforcement agent's use of a "beeper" concealed in a drum of chloroform to track a suspected drug manufacturer as he moved along public highways.[124] In considering Knotts's motion to suppress evidence

---

While a detailed discussion of the third party doctrine is beyond the scope of this Note, it is worth noting that jurists as prominent as Justice Sotomayor have recognized that straightforward application of the third party doctrine, as developed in the mid-twentieth century, may not be appropriate in the modern hyper-connected digital world:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. 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. Perhaps . . . some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I 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 protection.

United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

121 *See, e.g.*, Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475 (2012).

122 *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2635 (2010) (Scalia, J., concurring) (noting the difficulty in applying the Fourth Amendment to modern technology); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001).

123 460 U.S. 276 (1983).

124 *Id.* at 277.

gained from warrantless monitoring of the beeper, the Supreme Court held that, because traditional surveillance from public places could have revealed the suspect's location to the police, the defendant could not claim to have a reasonable expectation of privacy in his movements.[125] The fact that an (at the time) advanced technology was used to supplement law enforcement's surveillance effort was therefore constitutionally irrelevant.[126]

In *United States v. Karo*, decided two years after *Knotts*, the Supreme Court again considered the constitutionality of warrantless beeper tracking.[127] However, in *Karo* the Court was confronted with a question left open by *Knotts*—namely whether the otherwise unobjectionable use of the beeper became a Fourth Amendment search when it entered the suspect's home, an area "not open to visual surveillance."[128] This proved decisive for the Court, and served to remove the case from the conceptual framework established in *Knotts*. Recognizing that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight," the Court in *Karo* limited the application of *Knotts*, and held that a warrant is required where tracking technology would reveal location information that could not have otherwise been obtained without a warrant.[129]

These cases underscore the concept that an individual traditionally has no reasonable expectation of privacy in his movements in public spaces, which places monitoring these movements outside the purview of the Fourth Amendment.[130] However, as courts have often noted, "the Fourth Amendment protects people, not places."[131] At bottom, the

125 *Id.* at 281 ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

126 *Id.* at 282 ("The fact that the [police] . . . relied . . . on the use of the beeper . . . does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

127 United States v. Karo, 468 U.S. 705, 713–14 (1984).

128 *Id.* at 714. Critically, in *Knotts*, there had been no evidence that the beeper signal emanating from the drum containing the chloroform was monitored after it reached its destination. *Knotts*, 460 U.S. at 284–85.

129 *Karo*, 468 U.S. at 716. The officers in *Karo* did not rely primarily on visual surveillance, as they did in *Knotts*, but instead initially used a "strong beeper signal" to pinpoint its location inside a private home. *Id.* at 714. In doing so, they acquired information about the interior of the home that could not have been obtained by visual observation from outside the home. *Id.* at 715.

130 *Knotts*, 460 U.S. at 276–77.

131 Katz v. United States, 389 U.S. 347, 351 (1967).

Amendment is a tool to protect the public from excessive interference by law enforcement with individual rights.[132]

C. Maynard *and* Jones*: Tracking and the Fourth Amendment in the Modern Era*

The cases outlined above have provided the basic Fourth Amendment framework that has been utilized by contemporary courts when reviewing the warrantless use of location tracking technologies, including cell phones. However, it is worth noting that this body of precedent—running from *Katz* through *Knotts* and *Karo*—has been applied without substantial modification since the later part of the twentieth century.[133] Although these decisions might be considered to be of a relatively recent vintage in other areas of the law, when dealing with a field as technology- and context-specific as surveillance law, the passage of twenty or thirty years can significantly challenge many of the assumptions underlying the legal judgments rendered in these cases. This fact is clearly apparent in the most recent Supreme Court decision dealing with locational tracking.

In *United States v. Jones*, the Supreme Court held that attachment of a GPS tracking device to a suspect's vehicle without a warrant violated that individual's Fourth Amendment rights.[134] However, *Jones* is unique among recent locational privacy cases because it did not rely on the *Katz* test to reach this conclusion; instead it focused on the *Olmstead* rationale[135]—that law enforcement had trespassed on the suspect's property in affixing the tracking device to the undercarriage of Jones's vehicle.[136] This shift in focus is particularly interesting because the Court, in *Jones*, reviewed a D.C. Circuit decision that had applied the *Katz* test and held that the monitoring of the vehicle for twenty-eight days had violated the suspect's reasonable expectation of privacy *despite* the fact that the vehicle traveled exclusively on public roadways.[137]

---

132 *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 526 (2011) ("Most theories of the Fourth Amendment are premised on some sort of proper balance of police power.").

133 *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (holding that law enforcement use of a thermal imaging device to scan a private residence constituted a search through application of the *Katz* test).

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

135 *Id.* at 949–50, 952–54; *supra* note 117.

136 *Id.* at 948–49.

137 *Id.* The Court applied a concept known as the "mosaic theory" which previously pertained to the government's assertion of privilege in FOIA requests, to fashion a novel Fourth Amendment argument sometimes referred to as the "prolonged surveillance doctrine." United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010), *aff'd in part sub nom.*, *Jones*, 132 S. Ct. 945.

In deciding the case on these grounds, the Court declined to adopt the basis of the D.C. Circuit's holding that twenty-eight days of prolonged electronic surveillance in public spaces violated the *Katz* formulation of the Fourth Amendment.[138] Critically, however, the majority did not invalidate this approach, and explicitly left open the possibility that such a holding might be required in the near future.[139] Furthermore, it appears that a majority of the Court—the four dissenting Justices and Justice Sotomayor—was prepared to adopt some variation of the prolonged surveillance approach outlined by the D.C. Circuit.[140] Central to this rationale is the recognition that technological development upsets the balance of government power and individual liberty, and that the Fourth Amendment must evolve in order to maintain the baseline protection of privacy that existed when the Amendment was passed.[141]

IV. HISTORICAL CSLI CASES

As discussed in Part I, government requests for CSLI can encompass a variety of subclasses of data, for a wide durational range. While lower and intermediate courts have issued decisions regarding the legal protection afforded this data that are apparently starkly at odds with one another, nearly all have agreed that the relevant framework for

---

138 *Maynard*, 615 F.3d at 560 ("[T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil.").

139 *Jones*, 132 S. Ct. at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

140 As Justice Alito wrote:

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.

Id. at 964 (Alito, J., concurring).

141 *Id.* at 963 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."); *see also* United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) ("[T]he use of GPS technology [for] long-term tracking [may be] analogous to general warrants that the Fourth Amendment was designed to curtail, because of the technology's potential to be used arbitrarily or because it may alter the relationship between citizen and government in a way that is inimical to democratic society."), *judgment vacated*, 132 S. Ct. 1534 (2012) (mem.).

these cases is found in the cases discussed above.[142] However disparate these decisions may seem at first blush, this Part will argue that they generally agree that warrantless access to CSLI has at least the potential to violate the Fourth Amendment.

The crucial issue then becomes mapping out where exactly the fault lines lie between requests that do and do not violate the Fourth Amendment when unaccompanied by a warrant.[143] As this Part will demonstrate, much of the seeming disagreement between magistrate judges over the legal standard protecting CSLI can be traced back to differing conceptions of the current state of cell phone technology and differences among the underlying data requests they confront. When these differences are accounted for, a trend in favor of requiring a warrant for comprehensive requests emerges.[144] This Part will conclude with an attempt to cut through the confusion and provide some guidance as to when law enforcement requests for CSLI raise Fourth Amendment issues. In order to flush out the contours of this tentative consensus, the decisions must be disaggregated and considered based on two axes: (i) the comprehensiveness of the underlying request; and (ii) the duration of time the request covers.

A. *Comprehensiveness: How Limited Is the Government's Request?*

A court's opinion on whether access to CSLI intrudes upon constitutionally protected privacy interests may depend on the type of data that is requested and the judge's perception of how precise this data is for locational purposes. Therefore, even cases that have held the Fourth Amendment inapplicable to a particular request have generally not announced a blanket rule that historical CSLI can always be accessed without a warrant. For example, in *United States v. Suarez-Blanca*, although holding that the single tower data at issue was accessible under § 2703(d), the court explicitly noted "if the triangulation allows for tracking in private residences, then Fourth Amendment concerns might be implicated."[145]

---

142 *See, e.g.*, *In re* U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), C.R. Nos. C-12-755M, C-12-756M, C-12-757M, 2012 WL 3260215 (S.D. Tex. July 30, 2012) (compiling a comprehensive summary of cases that have divided on the legal protections appropriate to historical CSLI).

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

144 By "comprehensive," I mean to refer to requests which seek more than single tower data. For example, requests for cell-sector or multi-tower triangulation data would qualify as comprehensive.

145 United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *11 (N.D. Ga. Apr. 21, 2008).

In another notable example, the Third Circuit overturned a lower court holding that historical CSLI was always inaccessible without a warrant. This decision placed significant weight on the lack of evidence in the record indicating that *any* data from cell phones—including GPS data—could penetrate the interior of the home, and thereby implicate a warrant requirement under *Karo*.[146] It is worth pointing out that the proposition that GPS data can reveal an individual's location in the home is relatively uncontroversial, which seems to support reading the Third Circuit decision narrowly, as based more on a paucity of evidence below rather than a pronouncement about when historical CSLI will implicate the Fourth Amendment.[147] Other courts have been far more direct in their assessment of the precision of locational technology, opining that both triangulation and GPS data "unquestionably implicate Fourth Amendment privacy rights."[148]

In fact, when looked at closely, misunderstandings over the relative precision of CSLI explain many of the differing outcomes of CSLI cases. When courts feel that the requested data has the potential to reveal a suspect's location in his home, as in *Karo*, they have tended to find that the data request is improper without a warrant.[149] Conversely, where courts feel that the data is insufficiently precise, courts have frequently come out the other way and view *Knotts* as controlling.[150] As we have

---

146 *In re U.S. for an Order Directing a Provider*, 620 F.3d at 312–13 ("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, even when focused on cell phones that are equipped with GPS, extends to that realm. We therefore cannot accept the MJ's conclusion that CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production.").

147 While the Third Circuit left intact the ability of a magistrate judge to require a warrant, it indicated, albeit in dicta, that such option was to be exercised "sparingly." *Id.* at 319.

148 *In re* United States, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006); *see also* Freiwald, *supra* note 13, at 713 ("Courts apparently view triangulation . . . as constitutionally significant."). While the current state of technology is clearly at issue in these cases, differing views on the likely future advance of cell networks, and the appropriate judicial response to this development, also play a role. Judge Smith of the United States District Court for the Southern District of Texas has unequivocally acknowledged the influence of future technological development on his view that CSLI may never be accessed without a warrant, noting that the "inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year." *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010) (quoting *In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005)), *vacated*, 724 F.3d 600 (5th Cir. 2013).

149 The leading case is a 2010 opinion from the United States District Court for the Southern District of Texas, in which Magistrate Judge Smith's opinion found that "the level of detail provided by cell site technology now approaches that of GPS, and its reliability in obtaining a location fix actually exceeds that of GPS." *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 840 (questioning the constitutional significance of the distinction between historical and prospective cell data and holding that all such data was protected by the Fourth Amendment).

150 *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *11 (N.D. Ga. Apr. 21, 2008) ("In this case, the defendants have not shown that the government's

seen, the precision of the data requested is in turn directly related to the subclass of CSLI requested. Single tower data may be relatively imprecise (depending on the network technology), while cell sector data is comparatively more precise, and multi-site triangulation data is still more precise—approaching the accuracy of GPS.[151]

Courts have increasingly begun to take notice of these distinctions and should continue to do so.[152] An early case from the United States District Court for the Southern District of New York, although dealing with prospective CSLI, is illustrative.[153] In that case, the court reviewed a government request for cell sector data compiled during active use of a cell phone, finding that the request did not reveal constitutionally protected information because of its perceived lack of precision.[154] Notably, while placing the requested data outside the ambit of the Fourth Amendment, the court recognized that its ruling was dependent on the limited nature of the request, which concerned only single tower data collected when a call was made or received, and cautioned against an overly broad reading of its decision in light of rapid technological advances in this area.[155] Other magistrate judges have since pointed to this decision in support of the concept that limited requests for single-tower data collected during calls may be accessible under § 2703(d) with less than probable cause, while comprehensive requests that include triangulation data may not.[156] The Fifth Circuit, in the most recent decision to consider warrantless access to historical CSLI, likewise noted that the degree of comprehensiveness in government requests for CSLI may alter the constitutional analysis applied by a reviewing court.[157]

---

tracking of cell phone towers led to the tracking of the individual defendants in private quarters. Without such a showing, the Court cannot find any Fourth Amendment violation.").

151 *See supra* Part I.

152 *In re* U.S. for an Order, 411 F. Supp. 2d 678, 681 (W.D. La. 2006) (listing cases distinguishing between orders based on triangulation and those making less comprehensive requests).

153 *In re* U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

154 *Id.* at 449 ("The information does not provide a 'virtual map' of the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower." (citation omitted)).

155 *Id.* at 450 ("The above analysis applies with respect to the instant Order, and is based upon the technology that is available to the Government in this District. Because the [c]ourt cannot know how that technology may change, it intends to identify specifically, in any future orders authorizing the provision of cell site information, the character of the information that may be provided by a carrier.").

156 *See In re* U.S. for [an] Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 574 (W.D. Tex. 2010) (discussing distinctions in CSLI cases based on triangulation data); *see also In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 452 (S.D.N.Y. 2006) (noting a trend away from comprehensive requests).

157 *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

Although the Fifth Circuit held that a suspect lacks a reasonable expectation of privacy in CSLI generated when a call was placed or received, it expressly confined its Fourth Amendment analysis to this very limited class of data.[158] In so holding, the majority explicitly refused to decide whether the same considerations would apply to more comprehensive requests for "passive" historical CSLI, such as that collected merely by virtue of a phone being turned on and connected to the cell network.[159]

This contextual approach to historical CSLI makes eminent sense. The Department of Justice has conceded that prospective GPS data should be accessible only by a warrant showing probable cause.[160] Given the current state of technology, there is no reason to treat comprehensive requests for historical CSLI differently than those for GPS data for Fourth Amendment purposes. Both cell phone GPS and multi-tower CSLI have the potential to provide precise locational information revealing an individual's relative location within a residence that could not otherwise be ascertained without a warrant, in the process violating the reasonable expectation of privacy one enjoys in the home—and the Supreme Court's ruling in *Karo*.[161] Indeed, in cases where courts have properly conceptualized contemporary cell network technology—and realized that historical CSLI has the potential to achieve GPS-like accuracy[162]—courts have generally reached the conclusion that *Karo* provides the relevant precedent and held that comprehensive requests including triangulation and cell-sector data must be supported by a warrant.[163]

---

158 *Id.*

159 *Id.* ("Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address . . . orders requesting location information for the duration of the calls or when the phone is idle . . . .").

160 Letter from Rena Y. Kim, Chief, Freedom of Info./Privacy Act Unit, Office of Enforcement Operations, Criminal Div., to Catherine Crump, Staff Attorney, Am. Civil Liberties Union Found. (June 1, 2009), at 10–12, *available at* http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf (including excerpts from the U.S. Department of Justice training materials "pertaining to the use of mobile phone records for law enforcement purposes").

161 *See supra* notes 128–30 and accompanying text.

162 Some courts have responded to this uncertainty by simply refusing to issue a general rule regarding the application of the Fourth Amendment to cell location data, and preferred to allow access on the lesser § 2703(d) standard while leaving the determination of any constitutional violation to later review incident to a motion to suppress. *See In re* U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007); *see also* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008).

163 *See, e.g.*, *In re* U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011); *see also* Freiwald, *supra* note 13, at 712–13.

B. *Breadth of Requested Data: Applying Recent GPS Precedent to CSLI*

The other relevant variable when ascertaining the constitutionality of government access to CSLI is the length of time covered by the request. Law enforcement requests for historical CSLI can cover a broad range of time periods.[164] Occasionally the government will request data covering only a few days or weeks; generally, however, historical CSLI requests seek several months of data.[165] As a statutory matter, the SCA does not draw any distinctions based on the time period covered by these requests; however, the duration of a request is *constitutionally* significant. While early historical CSLI cases tended to be resolved based solely on a court's interpretation of the SCA to either allow or disallow warrantless access to historical data, after *United States v. Maynard*[166] and *United States v. Jones*, lower court judges have begun to recognize that prolonged, warrantless electronic surveillance violates the Fourth Amendment—even when it does not intrude on the constitutionally protected space of the home, as was required under *Knotts* and *Karo*.[167]

Those courts that have attempted to distinguish *Maynard* and *Jones* have generally not offered a persuasive rationale for doing so. For example, in *United States v. Graham*, a notable recent case decided in the United States District Court for the District of Maryland, the court permitted the government to access 221 days of historical CSLI data based on a § 2703(d) order.[168] The *Graham* court recognized that *Maynard* and the *Jones* concurrences could support a warrant

---

164 Because the SCA contains no temporal limitations on the amount that can be collected, in theory these requests are limited only by the collection and retention practices of the suspect's CSP. *In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) ("[T]he Stored Communications Act, unlike the Wiretap Act and the Pen Register Statute, does not limit the duration of law enforcement surveillance pursuant to a court order . . . .").

165 *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (allowing a request for 221 days of historical CSLI on a § 2703(d) order); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) (denying request for 113 days of CLSI).

166 United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010), *aff'd in part sub nom.*, United States v. Jones, 132 S. Ct. 945 (2012).

167 *See, e.g.*, *In re* U.S. for an Order Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. & Cell Site Info., 849 F. Supp. 2d 177, 179 (D. Mass. 2012) (noting Fourth Amendment concerns in light of *Maynard* and *Jones*, but allowing access to historical CSLI on a § 2703(d) order based on clear weight of precedent in that district); *In re* U.S. for an Order Authorizing Release of Historical Cell-Site Info., No. 11-MC-0113 (JO), 2011 WL 679925, at *1 (E.D.N.Y. Feb. 16, 2011) ("[A] month's worth of location tracking provides an intimate picture of the subject's life, and one that he does not meaningfully subject to public exposure, in part because sustained physical surveillance over such a period is effectively impossible."), *abrogated by In re* Smartphone Geolocation Data Application, No. 13-MJ-242 GRB, 2013 WL 5583711 (E.D.N.Y. May 1, 2013); *In re U.S. for an Order Authorizing the Release*, 809 F. Supp. 2d at 118 (denying government request).

168 *Graham*, 846 F. Supp. 2d 384.

requirement for this data; however, these decisions were ultimately distinguished. The *Graham* court highlighted that *Maynard* and *Jones* involved (i) GPS, as opposed to cell site data; and (ii) real-time tracking, as opposed to historical data.[169] Courts most commonly make these points when holding that CSLI is not protected by the Fourth Amendment. Unfortunately, neither supports the conclusion that a government request for over seven months of historical CSLI need not be supported by a warrant.

As Justice Sotomayor noted in *Jones*, law enforcement's use of inexpensive, invisible, and highly effective tracking devices on vehicles presents a serious Fourth Amendment issue because it upends the traditional, extra-legal forces that constrain police power.[170] Because CSLI now approaches GPS in precision, these concerns apply with at least as much force to law enforcement use of CSLI to achieve the same results as could be obtained through GPS tracking.[171] Indeed, because most people carry their cell phones on their person at all times,[172] historical CSLI may offer considerable benefits to law enforcement when compared to the GPS tracking used in *Jones*. This method of surveillance only traced the movements of the suspect's *vehicle* after law enforcement was able to physically attach the device.[173] With historical CSLI, on the other hand, law enforcement is able to gain access to an individual's past movements wherever his phone was connected to the network—whether he was in his car (or any other vehicle), on foot, or potentially even within his home or office—all without the need to attach or monitor a physical tracking device.[174]

---

169 *Id.* The court also relied on the third party doctrine, discussed *supra* note 120, to further distinguish *Maynard* and *Jones*. *Id* at 388.

170 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004))).

171 *See* Freiwald, *supra* note 13, at 712.

172 *See In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 589 (W.D. Pa. 2008) ("Our individual cell phones now come with us everywhere: not only on the streets, but in (a) business, financial, medical and other offices; (b) restaurants, theaters and other venues of leisure activity; (c) churches, synagogues and other places of religious affiliation; and (d) our homes and those of our family members, friends, and personal and professional associates."), *rev'd*, 620 F.3d 304 (3d Cir. 2010); *see also* AMANDA LENHART, PEW INTERNET & AM. LIFE PROJECT, PEW RESEARCH CTR., CELL PHONES AND AMERICAN ADULTS 2 (Sept. 2, 2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf ("65% of adults with cell phones say they have ever slept with their cell phone on or right next to their bed.").

173 *See In re* U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 543 (D. Md. 2011) (noting that tracking through a cell phone is likely to be more invasive and more problematic from a Fourth Amendment perspective, than GPS monitoring of a suspect's vehicle).

174 *Id.*

Due to the shrinking gap between the accuracy of GPS and network-based CSLI, decisions that find constitutional significance in the distinction between GPS and CSLI data are based on a misapprehension of the current state of cellphone technology.[175] Further, as many judges have indicated, the distinction between real-time tracking and historical data, as a Fourth Amendment matter, is also questionable.[176] Historical CSLI may in fact be more revealing—and more valuable to law enforcement—than prospective data.[177] Accordingly, the rule established in *Maynard* and the *Jones* concurrences should govern historical CSLI as well.

C. *Towards a Firm One Month Rule: Mapping* Maynard *and* Jones *to CSLI*

As the decision in *Graham* illustrates, many courts have struggled with the application of *Maynard* and *Jones* to historical CSLI, often due to an uncertainty about exactly when the Fourth Amendment becomes implicated.[178] Judges in these cases have appeared hesitant to announce a constitutional rule that draws seemingly arbitrary distinctions.[179] These judges often point out that determining bright-line rules regarding legal protection for historical CSLI is a task for the legislature, which is better suited to striking a delicate balance between the needs of law enforcement and the civil liberties of American citizens.[180] This fact may explain why relatively few judges have endorsed a clear constitutional rule that historical CSLI may *only* be accessed with a warrant.[181] Unfortunately, although frequently proposed and discussed, binding legislation on this issue has thus far not been forthcoming.[182]

---

175 Freiwald, *supra* note 13, at 712; *see supra* notes 70–72; *see also In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 838 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

176 *See, e.g.*, *In re* U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 585 (E.D.N.Y. 2010) ("The fact that the government seeks information that has already been created says nothing about whether its creator has a reasonable expectation of privacy in that information."), *rev'd*, Nov. 29, 2010; *In re* U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. & Historical Cell Site Info. for Mobile Identification Nos.: (XXX) XXX-AAAA, (XXX) XXX-BBBB, & (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 74–75 (D. Mass. 2007) ("Expecting a right to privacy in the location of where one is, or where one will be shortly, yet losing that expectation once leaving a location, is nonsensical." (footnote omitted)), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007).

177 *See* Freiwald, *supra* note 13, at 739–40 (arguing that historical and prospective CSLI should receive the same legal protection).

178 *In re U.S. for an Order Authorizing Release*, 736 F. Supp. 2d at 585.

179 *Id.*

180 *Id.*

181 *See, e.g.*, *In re* U.S. for an Order Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. & Cell Site Info., 849 F. Supp. 2d 177, 179 (D. Mass. 2012) ("[T]he privacy issues surrounding the collection of cumulative historical cell site location records are

While it may be true that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear,"[183] the judiciary risks far greater error when it makes no attempt whatsoever to apply the Fourth Amendment to novel surveillance practices.[184] Although a legislative solution to this issue may be preferable for any number of reasons,[185] in the meantime, courts have a duty to step into the fray and shield the public from government exploitation of the current confusion surrounding historical CSLI.[186]

Fortunately, for the vast majority of cases, concerns about premature or arbitrary rulemaking are misguided. In *Maynard*, the D.C. Circuit held that electronic surveillance of a vehicle over a one-month period violated the Fourth Amendment.[187] More importantly, five Justices on the Supreme Court—Justice Scalia for the majority, and Justices Alito, Ginsburg, Breyer, and Kagan concurring—have clearly indicated that they agree with this assessment.[188] Although courts are

---

best left to Congress—at least until the Supreme Court definitively considers the matter." (quoting United States v. Graham, 846 F. Supp. 2d 384, 405 (D. Md. 2012))).

182 *See* Pell & Soghoian, *supra* note 12, at 124 (noting the intractable nature of the debate between privacy advocates and law enforcement over appropriate reform of ECPA).

183 City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

184 As Magistrate Judge Orenstein of the United States District Court for the Eastern District of New York has noted:

> [B]y waiting too long to weigh in on the constitutionality of warrantless access to newly created kinds of information, the judiciary risks the error of transforming from mere assertion to self-fulfilling prophecy the government's contention that people categorically lack any reasonable expectation of privacy in [historical CSLI].

In re 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.

185 A legislative solution would have the ability to address additional problems with the current legal regime governing CSLI that courts are ill suited to handle, such as the absence of mandated notice to individuals who are being improperly monitored and a lack of "downstream" protections to data that is accessed by the government. For an in-depth discussion of these concepts, see Pell & Soghoian, *supra* note 12.

186 This is particularly true in light of the fact that much of the legislative action on this issue has been geared toward providing across-the-board warrant protections to CSLI. While these proposals are attractive from a privacy perspective, they are "non-starters" for the law enforcement community, which has used its substantial influence in Washington to bar any serious discussion of these bills. *See id.*

187 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.*, United States v. Jones, 132 S. Ct. 945 (2012).

188 As Justice Alito stated in his concurrence, which Justices Ginsburg, Breyer, and Kagan joined:

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify

only beginning to understand the impact of these recent decisions, magistrate judges in some jurisdictions have begun to recognize that individuals may claim a reasonable expectation of privacy in their "aggregate movement over a prolonged period of time."[189] This is a positive trend that should continue, as it provides an essential check on the previously unrestrained "all or nothing" scope of law enforcement access to historical CSLI while still permitting the government to make requests for a more targeted duration on the lower standard outlined in § 2703(d).[190]

The most powerful argument against this type of one-month rule is that it is inherently arbitrary—it is difficult to say why government access to three weeks of CSLI is unobjectionable, whereas the same access to five weeks of data constitutes a violation of one's reasonable expectation of privacy under the Fourth Amendment. This argument misses the point, however. Many constitutional rules are, by necessity, somewhat arbitrary at their core, yet this fact alone does not detract from their utility or prevent them from being accepted and validated over time.[191]

Moreover, because most historical CSLI cases concern time periods of many months, magistrate and district court judges need not confront the difficult question of when surveillance becomes a search—following *Maynard* and *Jones*, any request for historical CSLI covering a timeframe longer than one month is presumptively a search and should be supported by a warrant.[192] Magistrate judges who follow the D.C.

> with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.

Jones, 132 S. Ct. at 964 (Alito, J., concurring).

189 *In re* U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 543 (D. Md. 2011); *see also* United States v. Cuevas-Perez, 640 F.3d 272, 294 (7th Cir. 2011) (Wood, J., dissenting) ("Prolonged GPS surveillance, like a surreptitious wiretap, intrudes upon an individual's reasonable expectation of privacy by revealing information about her daily trajectory and patterns that would, as a practical matter, remain private without the aid of technology."), *judgment vacated*, 132 S. Ct. 1534 (2012) (mem.).

190 See Pell & Soghoian, *supra* note 12, for a legislative approach that would similarly accomplish this much needed minimization function regarding the scope of law enforcement requests.

191 As Judge Orenstein recently observed, "there is nothing new in the use of such prescriptive time periods to provide a bright-line rule to serve as useful guides for law enforcement officers seeking to perform their duties without running afoul of their targets' constitutional rights." *In re* U.S. for an Order Authorizing Release of Historical Cell-Site Info., No. 11-MC-0113 JO, 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011) (citing examples where constitutional rights are defined by arbitrary time periods), *abrogated by In re* Smartphone Geolocation Data Application, No. 13-MJ-242 GRB, 2013 WL 5583711 (E.D.N.Y. May 1, 2013).

192 Judge Orenstein has pursued this approach recently. *Compare In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (denying request for fifty-eight days of historical CSLI), *with In re U.S. for an Order Authorizing Release*, 2011 WL 679925 (allowing similar order for a twenty-one day period).

Circuit's approach in *Maynard* and insist on such a one-month rule will not act alone—a number of state supreme courts have likewise come to see that, due to its efficiency and secrecy, extended tracking of a suspect's location constitutes the type of twenty-four hour "dragnet surveillance" that the *Knotts* decision implied would require a different kind of Fourth Amendment analysis.[193]

CONCLUSION

We live in a time when technological engagement is not a choice, but an unavoidable fact of everyday life. Cell phones have rapidly evolved from mere modern conveniences to indispensable personal and professional tools.[194] As countless judges and academics have argued, it simply cannot be that those who wish to participate fully in modern life must first surrender their expectations of privacy in order to do so.[195] Judges would be wise to understand that comprehensive requests for all kinds of CSLI likely violate the principles laid down by the Supreme Court in *Karo*, which represents a positive trend that should be applied more broadly to historical CSLI requests. Moving forward, the judiciary must recognize that historical CSLI raises the same issues as prospective GPS tracking. Enforcement of the type of "one-month rule" discussed above would be vastly preferable to a system in which requests for historical CSLI covering the better part of a year are routinely granted based on a lesser standard than probable cause. Such a rule would lend a great deal of clarity to the current state of the law regarding historical CSLI. Moreover, unlike a uniform probable cause standard, this incremental step would likely curtail abuses of the current regulatory regime without unduly burdening law enforcement.[196]

---

193 United States v. Knotts, 460 U.S. 276, 283–84 (1983) (noting that its constitutional analysis of beeper tracking might be different if the prospect of abusive, twenty-four hour dragnet surveillance practices were to materialize); *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) (noting that "[c]onstant, relentless tracking of anything is now not merely possible but entirely practicable, indeed much more practicable than the surveillance conducted in *Knotts*" and holding that warrantless GPS monitoring therefore violated the New York State Constitution); State v. Campbell, 759 P.2d 1040, 1048–49 (Or. 1988); State v. Jackson, 76 P.3d 217, 224 (Wash. 2003).

194 City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

195 *In re U.S. for an Order Authorizing Release*, 736 F. Supp. 2d at 596 ("The Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society.").

196 The Department of Justice has adamantly opposed any attempt to impose such a standard by the judiciary or legislature. *See* Pell & Soghoian, *supra* note 12, at 123.