0091-4169/16/9106-0167
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 106, No. 2
 Printed in U.S.A.

CRIMINAL LAW

SMALL CELLS, BIG PROBLEMS: THE INCREASING PRECISION OF CELL SITE LOCATION INFORMATION AND THE NEED FOR FOURTH AMENDMENT PROTECTIONS

ROBERT M. BLOOM* & WILLIAM T. CLARK**

The past fifty years has witnessed an evolution in technology advancement in police surveillance. Today, one of the essential tools of police surveillance is something most Americans carry with them in their pockets every day, the cell phone. Cell phones not only contain a huge repository of personal data, they also provide continuous surveillance of a person's movement known as cell site location information (CSLI).

In 1986, Congress sought to provide some privacy protections to CSLI in the Stored Communication Act.[1] *Although this solution may have struck the proper balance in an age when cell phones were a mere novelty in the hands of a comparative few, we now live in an age where, as the U.S. Supreme Court recently recognized, cell phones could be seen "an important feature of human anatomy."*[2] *In 1986, there were only an estimated 681,825 subscribers serviced by 1531, cell sites. By 2013, there were 335 million subscribers and over 340,000 cell sites.*

* Professor of Law, Boston College Law School. I wish to thank Dana Borelli of the class of 2017 of Boston College Law School and Mark Schreiber of McDermott, Will, and Emory LLP for their valuable assistance.

** J.D. Boston College Law School (2015). William will be clerking for Douglas Woodlock Senior Judge U.S. District Court for the District of Massachusetts.

1 18 U.S.C. §§ 2701–2711.

2 Riley v. California, 134 S. Ct. 2473, 2484 (2014).

Recently, cell phone service providers have begun to use small cell technologies, miniature cell phone towers that can provide additional coverage and bandwidth support to overburdened cellular networks. Small cells, known variously as femtocells, picocells, and microcells, are already installed throughout the United States, in particular in urban areas. As small cells overtake traditional cell phone towers as the most common means of transmitting cellular signals, CSLI will transform from a means of placing a person's phone in a general area within a matter of miles to a precise location tracking tool charting a person's movements down to a matter of feet.

The late Justice Scalia in his 2001 majority opinion in Kyllo v. U.S.,[3] *a case involving thermal imaging, opined that "while the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."*[4]

This Article explores the evolution of CSLI by focusing on the rise of small cell technologies. It also canvasses decisions in the circuits involving CSLI. It points out that the third-party exception to the Fourth Amendment is inapplicable to CSLI. Following Justice Scalia's admonition, we believe that CSLI will only grow more precise as small cells infiltrate cellular networks and we therefore adopt an approach that incorporates the Fourth Amendment requirements for a search warrant particularly describing the place to be searched and items to be seized as well as the requirement for probable cause. Placing CSLI under the Fourth Amendment would make a major section of the Stored Communication Act unconstitutional.

TABLE OF CONTENTS

[3] 533 U.S. 27 (2001).

[4] *Id.* at 36.

INTRODUCTION

Dissenting from the U.S. Supreme Court's 1989 decision in *Florida v. Riley*,[5] Justice Brennan bemoaned the Court's choice to allow the government to observe a person's home via helicopter without a warrant.[6] Justice Brennan found it cause for concern that a four justice plurality of the Court was willing to "remove virtually all constitutional barriers to police surveillance" using this advanced technology.[7] To close his dissent, Justice Brennan invoked one of the most powerful stories of police surveillance in western culture: George Orwell's *1984*.[8] Noting the eerie parallel between the police surveillance methods at issue before the Court in *Riley* and Orwell's vision of government helicopters darting across the sky, Justice Brennan quoted the description of the infamous figure that loomed over Orwell's dystopian world: "The black-mustachio'd face gazed down from every commanding corner . . . . BIG BROTHER IS WATCHING YOU, the caption said . . . ."[9]

From a rudimentary tape recording device[10] to a sophisticated cell phone-computer,[11] the U.S. Supreme Court has struggled to balance the Fourth Amendment's protections against the steady technological

[5] 488 U.S. 445 (1989).

[6] *See id.* at 466 (Brennan, J., dissenting).

[7] *Id.*

[8] *Id*.

[9] *Id.* (quoting GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949)).

[10] *See* Katz v. United States, 389 U.S. 347 (1967).

[11] *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

advancements in police surveillance. The Court has confronted a wide range of surveillance technologies, from helicopters and heat rays to beepers and GPS trackers.[12] Today, however, the greatest threat to privacy is not the latest sophisticated government technology. It is a small rectangular box that resides in the pocket of nearly all Americans.

As the Court observed, cell phones, given their huge storage capacity, contain the sum of an individual's private life including photos, bank statements, videos, contacts, a literal trove of personal data, which the Court has sought to protect by requiring police to obtain a warrant before searching a cell phone.[13] But besides the intimate details contained therein, cell phones also invisibly chart the path of a person's movements throughout his or her day by generating what it is known as cell site location information (CSLI).[14]

Courts and scholars are split over whether police should obtain a warrant before reviewing CSLI.[15] Some view CSLI as blips of data generated and owned by private companies in the course of their business operations.[16] Under this view, police can review CSLI just as they could any other business record under the third-party doctrine exception.[17] Others view CSLI, when taken all together, as a rich tapestry that reveals deeply personal details of an individual's life.[18] Under this view, police can only review CSLI after obtaining a warrant because people have a fundamental privacy right against having their every movement tracked by the government despite technological evolutions.

Because of recent evolutions in cellular network technology, CSLI will soon paint an even more precise picture of a person's location history.[19]

---

[12] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 948 (2012); Kyllo v. United States, 533 U.S. 27, 29 (2001); Florida v. Riley, 488 U.S. at 447–48.

[13] *See* Riley v. California, 134 S. Ct. at 2494–95.

[14] *See infra* notes 39–42 and accompanying text (explaining how cell phones work and how CSLI is created).

[15] *Compare* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 690 (2011) (arguing that CSLI should receive Fourth Amendment protection), *with* Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 706 (2012) (arguing that the Fourth Amendment does not require the government to obtain a warrant before reviewing historical CSLI).

[16] *See, e.g.*, United States v. Davis (*Davis II*), 785 F.3d 498, 511 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

[17] *See id.*

[18] *See, e.g.*, United States v. Graham (*Graham I*), 796 F.3d 332, 345 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

[19] *See infra* notes 49–70 and accompanying text (discussing the rise of small cell

Cellular service providers, which have traditionally relied on large cell phone towers to send out signals, have started to add miniature cell phone towers known as "small cells" to their networks.[20] Small cells allow service providers to dramatically increase the number of cell towers in a particular area.[21] Although this provides many benefits to cell phone users, the increased concentration of cell towers means that CSLI will reveal a user's location down to a matter of feet instead of a matter of miles.[22]

This Article argues that the rise of small cells in cellular networks will make CSLI so accurate that it must fall under the Fourth Amendment's protection.[23] Part I discusses how cell phones operate relative to the collection of CSLI, the Fourth Amendment doctrines relevant to the collection of CSLI, and the current statutory framework by which the government obtains CSLI.[24] Part II reviews the current split amongst courts regarding whether the Fourth Amendment is applicable to CSLI.[25] Part III argues that the Fourth Amendment requires the government to obtain a particularized warrant supported by probable cause before reviewing CSLI.[26] Part III explains that the third-party doctrine, which has traditionally been regarded as an exception to the Fourth Amendment, does not apply to CSLI because people have a reasonable expectation of privacy in the detailed location history cell phones generate, unlike the information traditionally covered under the doctrine.[27]

I. A LOCATION TRACKER ON EVERY LAMPPOST: CSLI, SMALL CELLS, AND THE FOURTH AMENDMENT

This Part provides an introduction to CSLI and the Fourth Amendment.[28] Section A explains how cell phones work and how cell phone service providers increasingly employ small cell technologies to operate their networks.[29] Section B provides an overview of the Fourth Amendment principles relevant to CSLI, including the U.S. Supreme

technologies).

[20] *Graham I*, 796 F.3d at 350–51.

[21] *See infra* notes 49–70 and accompanying text (discussing the rise of small cell technologies).

[22] *Id.*

[23] *See infra* notes 231–278 and accompanying text.

[24] *See infra* notes 28–139 and accompanying text.

[25] *See infra* notes 140–230 and accompanying text.

[26] *See infra* notes 231–278 and accompanying text.

[27] *See infra* notes 252–268 and accompanying text.

[28] *See infra* notes 32–139 and accompanying text.

[29] *See infra* notes 32–70 and accompanying text.

Court's case law on location-based technologies and the third-party doctrine.[30] Section C provides an overview of the statutory limitations on the government's power to obtain CSLI.[31]

A. CSLI AND THE RISE OF SMALL CELL TECHNOLOGIES

1. Cell Phones and Traditional Cellular Networks

In December 1947, while working as an engineer in Bell Labs, Douglas H. Ring wrote an internal memorandum with the subject: "Mobile Telephony – Wide Area Coverage."[32] In his memorandum, Ring envisioned "[a] highly developed mobile telephone system" that would "ultimately be capable of providing service to a mobile unit from any part of the country at any place in the country."[33] His system would operate by precisely arranging radio transmitters in a hexagon honey-comb pattern, with three transmitters placed at the corners of each hexagon.[34] This would allow for the repeated use of certain frequencies with limited interference.[35]

Although it would take years for technology to catch up with his vision, Ring's proposal provided a significant foundation for our modern cellular networks.[36]

Modern cellular networks use base stations, also known as cell towers or cell sites, arranged in Ring's hexagon pattern to provide radio coverage to the largest amount of space in the most efficient manner.[37] Base stations are usually equipped with three antennas that each cover 120 degrees of area, thereby ensuring that each base station sends out signal in a complete circle.[38]

A cell phone connects to a base station whenever it places or receives a

---

[30] *See infra* notes 71–124 and accompanying text.

[31] *See infra* notes 125–139 and accompanying text.

[32] Alexis C. Madrigal, *The 1947 Paper That First Described a Cell-Phone Network*, THE ATLANTIC (Sept. 16, 2011), http://www.theatlantic.com/technology/archive/2011/09/the-1947-paper-that-first-described-a-cell-phone-network/245222/.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *See id.*; *see also* JON AGAR, CONSTANT TOUCH: A GLOBAL HISTORY OF THE MOBILE PHONE, 19–22 (2d ed. 2004), https://www.ucl.ac.uk/sts/staff/agar/documents/agar_constant touch.

[37] Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. ATT'Y BULL 16, 19 (2011), http://www.justice.gov/usao/eousa/foia_reading_ room/usab5906.pdf.

[38] *Id.* at 27.

call or text message.[39] When a cell phone connects to the base station, it provides the user's telephone number as well as other information, including the device's International Mobile Equipment Identifier,[40] a unique number that identifies the particular cell phone (like a VIN number for cars). The wireless service provider, which maintains the cellular network, records which cell phone connected to the network, when it connected, and through which base station it connected in order to bill the account associated with that device.[41] This information is known generally as CSLI.[42]

The rapid rise of smartphones and other mobile computing devices has threatened to overload the traditional cellular network.[43] In 2012, Americans used 1.468 trillion megabytes of data annually.[44] In 2014, that number more than doubled, as Americans used 4.06 trillion megabytes of data annually.[45] Moreover, each year more and more people are turning away from laptop and desktop computers to rely almost exclusively on their mobile devices.[46] Some predict that by 2017, mobile devices will be the

[39] *Graham I*, 796 F.3d 332, 343 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

[40] O'Malley, *supra* note 37, at 20.

[41] *Id*. at 23.

[42] CSLI comes in two discrete forms: real-time and historic. This Article focuses on historic CSLI, as it is the Fourth Amendment's application to this information that has divided courts. *See* Malone, *supra* note 15, at 710 (discussing the difference between historic and real-time CSLI and observing that "[a] majority of courts" have required warrants based on probable cause for orders for real-time CSLI).

[43] *See CTIA-The Wireless Association Survey Shows Americans Used 26 Percent More Wireless Data in 2014*, CTIA (Jun. 17, 2015), http://www.ctia.org/resource-library/press-releases/archive/ctia-survey-shows-americans-used-26-percent-more-wireless-data-in-2014 (stating that "[t]he year-over-year pressure of skyrocketing mobile data and device growth highlights the need for a long-term national spectrum plan so that Americans continue to enjoy new and innovative wireless offerings").

[44] *See* Mike Dano, *CTIA: U.S. wireless network traffic reaches 1.468 trillion MB in 2012*, FIERCE WIRELESS (May 2, 2013) http://www.fiercewireless.com/story/ctia-us-wireless-network-traffic-reaches-1468-trillion-mb-2012/2013-05-02 (stating that "CTIA today released its semi-annual survey, showing that wireless network data traffic in the United States rose 69.3 percent in 2012 from 2011. The firm said the total amount of megabytes traveling over U.S. wireless networks in 2012 reached 1.468 trillion, up from 866.8 billion in 2011.").

[45] CTIA, *supra* note 43.

[46] SMALL CELL FORUM, SMALL CELLS–WHAT'S THE BIG IDEA? 1 (2014), http://scf.io/en/documents/030_-_Small_cells_big_ideas.php (hereinafter "WHAT'S THE BIG IDEA?"); Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015) http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

primary generators of all Internet traffic,[47] thus the need for more CSLI locations and technology which is discussed in the next Section. In order to address these growing capacity challenges, many service providers are turning to small cell technologies.[48]

2. Small Cell Technology and the Growing Precision of CSLI

Small cells are miniature base stations that provide a small range of cellular signal in areas that are either overburdened or underserved by traditional cellular networks.[49] Small cells typically have a range of nine meters (about thirty feet) to several hundred meters as compared to traditional cell towers, which cover several "tens of kilometers."[50] Small cells can serve urban communities, where the high population density puts a massive strain on the network, or rural communities where installing a large base station would not be cost-effective.[51] Small cells have many different names based on their different functions and uses, including femtocells, picocells, microcells, and metrocells.[52]

Femtocells are compact base stations, some about the size of a broadband router, developed for residential use.[53] For those who have poor cell phone coverage at home, femtocells put a cell phone tower into the home itself.[54] Several major wireless networks, including Verizon and AT&T, sell femtocells directly to consumers for use in their homes for approximately two hundred fifty dollars.[55]

Picocells are another form of small cell technology developed for commercial or public use.[56] For example, picocells can be installed in high-

[47] WHAT'S THE BIG IDEA?, *supra* note 46, at 1.

[48] *Id.* at 1–2.

[49] *Id.* at 3.

[50] *Id.*

[51] *Id.*

[52] WHAT'S THE BIG IDEA?, *supra* note 46, at 1.

[53] Jeffrey G. Andrews et al., *Femtocells: Past, Present, and Future*, 30 (3) IEEE J. ON SELECTED AREAS IN COMMUNICATIONS, 497 (Apr. 2012); WHAT'S THE BIG IDEA?, *supra* note 46, at 3.

[54] WHAT'S THE BIG IDEA?, *supra* note 46, at 3.

[55] *See, e.g.*, VERIZON, SAMSUNG NETWORK EXTENDER (SCS-2U01), http://www.verizonwireless.com/accessories/samsung-network-extender-scs-2u01/ (last visited Jul. 23, 2016) (marketing its network extender as "a miniature cell phone tower" and listing its price at $249.99); AT&T, AT&T MICROCELL, http://www.att.com/att/microcell/ (last visited Jul. 23, 2016) (advertising its femtocell as "a mini cellular tower, boosting cellular performance in your home or small business").

[56] WHAT'S THE BIG IDEA?, *supra* note 46, at 3; FUJITSU, HIGH-CAPACITY INDOOR WIRELESS SOLUTIONS: PICOCELL OR FEMTOCELL? 2 (2013) https://www.fujitsu.com/us/

network demand locations, such as hotels, large office buildings, or even sports arenas, in order to offload some of the demand placed on the traditional network.[57] Microcells are a similar technology more appropriate for outdoor use.[58]

Finally, small cell technologies used in dense urban areas are sometimes referred to as metrocells.[59] Metrocells can address signal issues in so-called "urban canyons"—narrow streets where tall buildings may obstruct signal.[60] Metrocells are often hidden in plain sight on city streets, attached to streetlights, building walls, or even security camera poles.[61]

Given the wide variety of small cells and the different advantages they provide, service providers have increasingly incorporated them into their networks. In 2011, it was estimated that there were 2.3 million femtocells in use globally.[62] For 2015, industry analysts expected 4 million small cells to ship and projected that number to reach 8 million per year by 2019.[63] Verizon and AT&T are projected to add approximately 100,000 small cells in the United States in 2016.[64] According to one report, by 2020, 40% of small cells will be deployed in hyper-dense networks, where there will be more than 150 small cells concentrated in one square kilometer.[65]

Service providers have begun to partner with municipalities to install small cells. Verizon recently announced that it would place 400 small cells

Images/High-Capacity-Indoor-Wireless.pdf.

[57] WHAT'S THE BIG IDEA?, *supra* note 46, at 3; Jeffrey Spivak, *Raising the (Phone Coverage) Bars in Commercial Buildings*, URBAN LAND (May 12, 2014), http://urbanland.uli.org/infrastructure-transit/raising-phone-coverage-bars-commercial-buildings/ (describing how owners of commercial real estate are integrating picocells and other small cell technologies into their buildings).

[58] WHAT'S THE BIG IDEA?, *supra* note 46, at 3.

[59] *Id.*

[60] *Id.*; FUJISTSU, *supra* note 56, at 2.

[61] WHAT'S THE BIG IDEA?, *supra* note 46, at 3; Chuck Soder, *'Small Cells' are One of the Next Big Things for Carriers*, CRAIN'S CLEVELAND BUSINESS (Apr. 13, 2015), http://www.crainscleveland.com/article/20150412/SUB1/304129979/small-cells-are-one-of-the-next-big-things-for-carriers (discussing Verizon's placement of small cells on street lights and utility poles in Cleveland).

[62] Andrews et al., *supra* note 53, at 497.

[63] SMALL CELL FORUM, SMALL CELLS DEPLOYMENT MARKET STATUS REPORT (2015), http://scf.io/en/documents/050_-_Market_status_report_June_2015_-_Mobile_Experts.php.

[64] Martha DeGrasse, *Can Verizon and AT&T Deploy 100,000 New Small Cells?*, RCR WIRELESS NEWS (Oct. 29, 2015), http://www.rcrwireless.com/20151029/carriers/can-verizon-and-att-deploy-100000-new-small-cells-tag4.

[65] SMALL CELL FORUM, CROSSING THE CHASM: SMALL CELLS INDUSTRY (2015), http://scf.io/en/white_papers/Crossing_the_Chasm_Small_Cells_Industry_2015.php.

on utility poles throughout San Francisco.[66] Similarly, Los Angeles has announced a partnership with Ericsson, a European telecommunications company, to install 100 "SmartPoles," streetlights that will incorporate small cell technology.[67] The Federal Communications Commission (FCC) has also recently updated its rules on cellular networks to promote the installation of small cells.[68] The FCC reformed its environmental and historic preservation rules in order to ensure that small cell technologies would be able "to flourish, delivering more broadband service to more communities."[69]

The integration of small cell technologies into cellular networks will make CSLI increasingly precise. Because CSLI generated from small cells could reveal a cell phone user's location to within fewer than ten feet, such CSLI would be more accurate than location data generated from GPS technologies, which can determine location to within only fifty feet.[70] Recognizing the growing threat to privacy that CSLI presents, courts have struggled with how to best apply both constitutional and statutory protections to this information.

B. THE FOURTH AMENDMENT AND LOCATION TRACKING

The Fourth Amendment provides two essential protections. First, it enshrines "[t]he right of the people to be secure . . . against unreasonable searches and seizures."[71] Second, it limits the power of courts to grant

---

[66] Martha DeGrasse, *Verizon Explains Rollout of Small Cells*, RCR WIRELESS NEWS (July 29, 2015), http://www.rcrwireless.com/20150729/network-infrastructure/verizon-explains-small-cell-rollout-tag4. One resident protested Verizon's proposed location for a new small cell, expressing concern that "the antenna is on the pole ten feet in front of my house." CBS SF BAY AREA, *SF Residents Battle Wireless Firms Over Super Bowel Building Boom*, (Oct. 31, 2015), http://sanfrancisco.cbslocal.com/2015/10/31/san-francisco-residents-battle-wireless-companies-cell-tower-building-boom-super-bowl-fifty/.

[67] Aaron Tilley, *Los Angeles Becomes First City to Test the Future of Wireless Connectivity with 'Small Cells' on Streetlights* (Nov. 5, 2015), http://www.forbes.com/sites/aarontilley/2015/11/05/los-angeles-becomes-first-city-to-test-the-future-of-wireless-connectivity-with-small-cells-on-streetlights/#52196ae653ad.

[68] *In the Matter of Acceleration of Broadband Deployment by Improving Wireless Facilities Siting Policies*, 29 F.C.C. Rcd. 12865, No. 16 (2014).

[69] *Id.* at 12876.

[70] United States v. Carpenter, Nos. 14-1572, 14-1805, 2016 WL 1445183, at *9 (6th Cir. Apr. 13, 2016) (describing the accuracy of GPS data); Stephanie K. Pell & Christopher Soghoain, *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, 132 (2012).

[71] U.S. CONST. amend. IV.

warrants, allowing warrants to issue only when the government establishes "probable cause . . . and particularly describ[es] the place to be searched, and the persons or things to be seized."[72] The particularity requirement was designed by the Founding Fathers to combat the use of general warrants by English Customs Officers which allowed them to search anywhere they wanted for uncustomed goods.[73]

There are two different theories for determining whether a "search" has occurred within the meaning of the Fourth Amendment: the trespass theory and the privacy theory.[74] Under the trespass theory, the government searches only when it physically intrudes upon certain recognized property interests.[75] For many years, the trespass theory was the only way to establish a search under the Fourth Amendment.[76]

In the 1967 landmark decision of *Katz v. United States*,[77] the U.S. Supreme Court introduced a new vision of the Fourth Amendment based not in property rights, but in privacy rights.[78] In *Katz*, the defendant entered a telephone booth and called someone to place a bet.[79] The government, having installed a listening device on the telephone booth, recorded his conversation, and Katz was later convicted of illegal gambling.[80] The Court held that recording the defendant's conversation violated his Fourth Amendment rights.[81] Although the Court noted that the government had not trespassed against the defendant's property, it found that the Fourth Amendment protects whatever information a person "seeks to preserve as private, even in an area accessible to the public."[82] The Court was willing to recognize the defendant's asserted privacy right because people

---

[72] *Id.*

[73] *See* Groh v. Ramirez, 540 U.S. 551 (2004).

[74] United States v. Davis (*Davis I*), 754 F.3d 1205, 1212–13 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014) *and on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015) *cert. denied*, 136 S. Ct. 479 (2015) (discussing the two theories of Fourth Amendment searches and their history).

[75] *See* United States v. Jones, 132 S. Ct 945, 949–50 (2012).

[76] *See id.* (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)); Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004) ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

[77] 389 U.S. 347 (1967).

[78] *Id.* at 353; *see also* Olmstead v. United States, 277 U.S. 438, 464 (1928), *overruled by Katz*, 389 U.S. at 353.

[79] *Katz*, 389 U.S. at 348.

[80] *Id.*

[81] *Id.* at 347.

[82] *Id.* at 347, 352–53.

reasonably expect that, when they enter a telephone booth, their phone call "will not be broadcast to the world."[83] The Court sought to extend the Fourth Amendment's protections to phone calls in telephone booths in part because of "the vital role that the public telephone has come to play in private communication."[84]

Concurring in *Katz*, Justice Harlan proposed a two-step privacy-based test for assessing Fourth Amendment claims, which has become the modern standard for claims brought under the privacy theory.[85] First, the Court examines whether a person has "exhibited an actual (subjective) expectation of privacy" in the place or information at issue.[86] Second, the Court decides whether that expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[87] If both conditions are met, then a Fourth Amendment search has occurred and, barring an exception to the contrary, a warrantless search of such information will be deemed improper.[88] In addition, probable cause would also be required.

The Court has struggled to determine when and where society will recognize a reasonable expectation of privacy, particularly in the face of technological evolutions. In a pair of 1980s cases, the Court grappled with beeper technology, an early location-tracking tool.[89] In 1983, the Court held in *United States v. Knotts* that the police did not violate the defendant's Fourth Amendment rights by using a beeper to track his journey along public roads from the scene of a drug purchase to an associate's house.[90] The Court observed that the same tracking could have been accomplished through visual surveillance alone.[91] The Court recognized the defendant's argument that such a narrow view of the Fourth Amendment would allow "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision."[92] But the Court found that the surveillance at issue in this case was quite limited in duration (from one location to another) and stated that "if such dragnet-type law enforcement

---

[83] *Id.* at 352.

[84] *Id.*

[85] *Id.* at 361 (Harlan, J., concurring); *see also* United States v. Jones, 132 S. Ct. 945, 950 (2012) (noting how "later cases have applied the analysis of Justice Harlan's concurrence").

[86] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[87] *Id.*

[88] *Id.*

[89] United States v. Karo, 468 U.S. 705, 707 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).

[90] *Knotts*, 460 U.S. at 281–82.

[91] *Id.* at 282.

[92] *Id.* at 283.

practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[93]

In 1984, the Court in *United States v. Karo* placed a key limitation on the use of location-tracking technology. In *Karo*, just as in *Knotts*, the government used a concealed beeper to track the movements of the defendant.[94] Unlike in *Knotts*, the government continued to monitor the beeper after it had been placed in the defendant's house.[95] The Court found that this in-home tracking went beyond what the government could have visually observed from public streets, for the beeper told the government "that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched."[96] To the Court, this information "reveal[ed] a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant."[97] Therefore, the Court held the use of the beeper violated the defendant's reasonable expectation of privacy in his whereabouts while out of public sight in his home.[98] It should be pointed out that the home enjoys the greatest Fourth Amendment protection.[99]

Nearly thirty years later, the Court fractured over how to bring the next generation of location-tracking technology into the Fourth Amendment's purview. In 2012, the Court in *United States v. Jones*[100] unanimously found that when the government tracked the defendant using a GPS device it installed on his vehicle, it had "searched" the defendant within the meaning of the Fourth Amendment.[101] The majority explicitly declined to determine whether the defendant had a reasonable expectation of privacy in the GPS location information.[102] Instead, the majority returned to the pre-*Katz* trespass doctrine and emphasized the fact that the government had physically attached the GPS device to the vehicle, holding that when "the Government obtains information by physically intruding on a

---

[93] *Id.* at 284.

[94] *Karo*, 468 U.S. at 707–08.

[95] *Id.* at 714.

[96] *Karo*, 468 U.S. at 715.

[97] *Id.*

[98] *Id.* at 716.

[99] *See generally* Kyllo v. United States, 533 U.S. 27 (2001)

[100] 132 S. Ct 945 (2012).

[101] *Id.* at 949, 957–58 (Alito, J., concurring in the judgment).

[102] *Id.* at 947 (majority opinion) (noting how the defendant's Fourth Amendment rights do not rise or fall with the *Katz* formulation).

constitutionally protected area . . . a search has undoubtedly occurred."[103]

Justice Alito took issue with the majority's reliance on the archaic trespass theory of the Fourth Amendment in a concurrence joined by Justices Ginsburg, Breyer, and Kagan.[104] Justice Alito asserted that *Katz* "did away with" the trespass theory of the Fourth Amendment, leaving the privacy approach as the exclusive framework.[105] Justice Alito, however, struggled to explain what amount of location tracking triggered the Fourth Amendment's protection by violating a defendant's reasonable expectation of privacy. Justice Alito noted the continued applicability of *Knotts*, stating that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[106] But, he found that the "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[107] Acknowledging the doctrinal tension of applying the Fourth Amendment in this context, Justice Alito invited Congress to enact new regulations that could better respond to these technological advances.[108]

Justice Sotomayor joined the majority opinion, but wrote separately to discuss the consequences of precise location tracking in the modern age.[109] Justice Sotomayor emphasized how location tracking through GPS technology allowed the government to not only create "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," but also to retain this record indefinitely.[110] To Justice Sotomayor, such extensive monitoring by the government "chills associational and expressive freedoms."[111] Justice Sotomayor stated that all of these considerations should weigh on the Court's evaluation of the defendant's asserted privacy right under *Katz*.[112]

Justice Sotomayor used her concurrence to critique one of the most controversial theories in Fourth Amendment jurisprudence: the third-party

---

103 *Id.* at 950.
104 *See Jones*, 132 S. Ct. at 949.
105 *Id.* at 959–60 (Alito, J., concurring in the judgment).
106 *Jones*, 132 S. Ct. at 964.
107 *Id.*
108 *Id.* at 963–64.
109 *Id.* at 954–57 (Sotomayor, J., concurring).
110 *Id.* at 955–56.
111 *Id.* at 956.
112 *Id.*

doctrine.[113] The third-party doctrine establishes that one cannot have a reasonable expectation of privacy in information that he or she has given to a third party voluntarily.[114] In 1976, the Court in *United States v. Miller* held that the government did not violate the Fourth Amendment when it obtained the defendant's financial records held at his bank without a warrant because the defendant had voluntarily given these records to the bank.[115] Similarly, in 1979, the Court in *Smith v. Maryland* held that the government's use of a pen register, a technology which records the phone numbers dialed on a phone, did not violate the Fourth Amendment because the defendant voluntarily provided the phone company with these phone numbers by placing the call.[116] In both of these cases, the Court linked the third-party doctrine to the reasonable expectation of privacy test, observing in *Smith* that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[117]

In her *Jones* concurrence, Justice Sotomayor argued that the third-party doctrine should be revisited, as she viewed the doctrine "ill suited to the digital age."[118] Justice Sotomayor observed that in today's world, people disclose a great deal of information to third parties that many in society would still likely consider private, such as "the URLs that they visit and the e-mail addresses with which they correspond."[119] Justice Sotomayor stated that she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[120]

Finally, the Court has recently recognized the essential role cell phones have in modern society in its 2014 decision in *Riley v. California*.[121] Observing that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy," the Court unanimously held that the government must obtain a warrant before searching a cell phone.[122] Although the common law had allowed police to search the items on an

---

[113] *Id.* at 957.

[114] Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976); *see also* Hoffa v. United States, 385 U.S. 293, 301–02 (1966).

[115] *Miller*, 425 U.S. at 442.

[116] *Smith*, 442 U.S. at 744.

[117] *Smith*, 442 U.S. at 743–44.

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

[119] *Id.*

[120] *Id.*

[121] Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

[122] *Id.* at 2484.

arrestee's person for centuries, the Court found that this traditional approach did not strike the right balance between the government's interests and arrestee's privacy interests when applied to cell phones.[123] Concurring in *Riley*, Justice Alito again invited Congress and states to pass new regulations on cell phone searches, asserting that legislatures may be the better equipped to balance the competing interests at stake.[124]

C. THE ARCHAIC PROTECTIONS OF THE STORED COMMUNICATIONS ACT

Along with the constitutional limitations courts have imposed on searches assisted by modern technology, Congress has also placed limits and established procedures for such searches. In fact, Congress and the Court have often worked hand-in-hand to bring privacy protections to evolving technologies. For example, in 1968, after the Court brought audio surveillance within the purview of the Fourth Amendment in *Katz*, Congress passed the Wiretap Act, which sought to regulate the government access to the contents of traditional phone calls.[125] The Act provided for comprehensive and detailed regulations and procedures for wiretap orders.

In 1986, Congress enacted the Electronic Communications Privacy Act, which included a subsidiary act called the Stored Communications Act (SCA).[126] Then, in 1994, Congress updated the SCA and established the current standards governing law enforcement requests for electronic communications.[127] For historic CSLI, the SCA permits the government access through two different court orders. First, the government may obtain a warrant that meets the standards of both the Federal Rules of Criminal Procedure and the Fourth Amendment.[128] Under this approach, a judge must find that there is probable cause to support the warrant.

Second, the government may obtain a court order which requires a

---

[123] *Id.*

[124] *Id.* at 2497 (Alito, J, concurring in part and concurring in the judgment).

[125] Wiretap Act, 18 U.S.C. § 2510 (2012); DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 264–65 (2d ed. 2006).

[126] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2510 *et seq*.); Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. § 2701 *et seq.)*; SOLOVE ET AL., *supra* note 125, at 265.

[127] *See In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 314 (3d Cir. 2010) (reviewing the history of the SCA); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219 (2004).

[128] 18 U.S.C. § 2703(c)(1)(A) (2016).

lower showing than probable cause.[129] Although the court order is similar to the warrant requirement of the Fourth Amendment, in that a neutral detached judicial officer is determining the justification, the amount of justification distinguishes it from the traditional warrant requirement. Under § 2703(d) of the SCA, the government can obtain a court order for CSLI if it "offers specific and articulable facts showing that are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[130] This standard is based off the U.S. Supreme Court's reasonable suspicion standard, which originated in *Terry v. Ohio*.[131] In *Terry*, the Court adopted a lesser standard than probable cause because the intrusion, a pat-down by a police officer, was somewhat less than an arrest[132] and because at the time the legislation was passed location data was imprecise and there were substantially fewer cell phones. In the same way, Congress at the time believed CSLI did not need the full protection of probable cause because the review of CSLI did not seriously impinge on a cell phone user's privacy.[133]

Section 2703(d)'s standard places a less stringent burden on the government both in its evidentiary showing and in its target. Since *Terry*, courts have routinely recognized that a showing of "reasonable suspicion" is easier to meet than a showing of probable cause.[134] Moreover, because the government must only show that the information is "relevant and material" to the investigation, it can obtain § 2703(d) orders with a far broader scope than a Fourth Amendment warrant, which requires particularized descriptions of the place to be searched and the items to be seized.[135] These lower standards have allowed the government to seek out CSLI at an alarming rate. In 2015, AT&T received 58,189 demands for historic CSLI, while in the second half of 2015, Verizon received 20,298 demands for CSLI, two-thirds of which came from § 2703(d) orders.[136]

---

[129] *Id.* § 2703(a).

[130] *Id.* § 2703(d).

[131] Terry v. Ohio, 392 U.S. 1, 30 (1968).

[132] *Id.*

[133] *See In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 314–15 (3d Cir. 2010), (discussing how the legislative history of the SCA and its amendments show that the government sought an "intermediate [standard] that is less stringent than probable cause").

[134] *See, e.g.*, United States v. Cortez, 449 U.S. 411, 421 (1981).

[135] Freiwald, *supra* note 15, at 697.

[136] *AT&T Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited July 9, 2016); *Verizon Transparency Report*, VERIZON, http://www.verizon.com/about/portal/transparency-

When the SCA was passed, cell phones were still very much in their infancy. The FCC had permitted the first generation of cellular service networks only five years before.[137] In 1986, there were only an estimated 681,825 total subscriber connections in the United States serviced by 1,531 cell sites.[138] In contrast, by 2013, there were over 335 million estimated total subscriber connections, in turn serviced by 304,360 cell sites.[139] Due to this explosion in cell users and cell sites, CSLI is no longer an imprecise means of tracking available in only a few parts of the country; CSLI has created a dragnet surveillance system far beyond what the legislators who enacted the SCA could have imagined.

II. AN INDIVIDUAL'S PERSONAL HISTORY OR A SERVICE PROVIDER'S BUSINESS RECORD?: COURTS SPLIT OVER FOURTH AMENDMENT'S APPLICATION TO CSLI.

The initial circuit courts to address the Fourth Amendment's application to CSLI found that the government's warrantless review of such information did not violate the Fourth Amendment. In 2010, the Third Circuit Court of Appeals held that the government did not have to show probable cause to obtain a court order for CSLI.[140] The Third Circuit distinguished CSLI from the beeper technology used in *Knotts* and *Karo*, finding that CSLI was less precise than beeper tracking technology and therefore did not raise the same level of privacy concerns.[141] Then, in 2013, the Fifth Circuit Court of Appeals relied on the third-party doctrine to hold that those who use cell phones voluntarily convey their location to their phone providers and therefore have no reasonable expectation of privacy in the CSLI generated.[142]

Recently, however, courts have begun to fracture over this question. This Part reviews the recent evolution in case law on CSLI and the Fourth Amendment.[143] Section A discusses the courts that have found that a

report/us-report/ (last visited July 9, 2016).

[137] *See Cellular Communications Systems Decisions*, 86 F.C.C.2d 469 (1981).

[138] *See* Cellular Telecomm. Indus. Ass'n, Annual Wireless Industry Survey Results—December 1985 to December 2013 (2014), http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2013_graphics-final.pdf?sfvrsn=2.

[139] *Id.*

[140] *In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 313 (3d Cir. 2010).

[141] *Id.* at 312.

[142] *In re* United States for Historical Cell Site Data, 724 F.3d 600, 613–14 (5th Cir. 2013).

[143] *See infra* notes 147–230 and accompanying text.

warrantless review of CSLI violates the Fourth Amendment.[144] Section B discusses the courts that either have found that the Fourth Amendment does not apply to CSLI or have yet to firmly decide.[145]

A. COURTS THAT HAVE HELD THAT THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT BEFORE REVIEWING CSLI

In 2014, the Eleventh Circuit Court of Appeals in *United States v. Davis* (*Davis I*),[146] became the first circuit to hold that the Fourth Amendment requires the government to obtain a warrant before reviewing CSLI.[147] In *Davis I*, the government received a court order for CSLI on the defendant, and then used that CSLI to show that the defendant had made phone calls at the same time and location as several robberies.[148] The Eleventh Circuit held that the defendant had a reasonable expectation of privacy in the CSLI generated from his cell phone.[149] The court compared the warrantless GPS tracking of a car in *Jones* to the tracking of a cell phone through CSLI.[150] The court found that tracking a cell phone can invade a person's privacy far more than tracking a car, for "[o]ne's cell phone, unlike an automobile, can accompany its owner anywhere . . . convert[ing] what would otherwise be a private event into a public one."[151] Moreover, the Eleventh Circuit rejected the government's argument that CSLI was too imprecise to violate a reasonable expectation of privacy.[152] To the court, even if CSLI could only reveal whether a person is near a location, "[t]here is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."[153]

The Eleventh Circuit also found that the third-party doctrine did not apply because the defendant had not voluntarily conveyed his location to

---

144 *See infra* notes 147–188 and accompanying text.

145 *See infra* notes 189–230 and accompanying text.

146 *Davis I*, 754 F.3d 1205, 1217 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014) *and on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

147 *Id.*

148 *Davis I*, 754 F.3d at 1209–10, 1218.

149 *Id.* at 1215.

150 *Id.* at 1216.

151 *Id.*

152 *Id.*

153 *Id.*

his cell phone provider.[154] The court recognized that most cell phone users would not think that their service providers both collect and, more importantly, "*store historical location information.*"[155] The court recounted the prosecutor's statement to the jury in the defendant's trial, where he said the defendant and his co-conspirators "probably had no idea that by bringing their cell phones with them to these robberies they were allowing [their cell service provider] and now all of you to follow their movements on the days and at the times of the robberies."[156]

In 2015, a divided panel of the Fourth Circuit Court of Appeals in *United States v. Graham* (*Graham I*)[157] held that the government's warrantless collection and review of a person's CSLI violates the Fourth Amendment.[158] In *Graham*, the government received a list of the defendant's CSLI from July 1, 2010 through February 6, 2011, a period of 221 days.[159] The Fourth Circuit noted that "[t]he Supreme Court has recognized an individual's privacy interests in comprehensive accounts of her movements, in her location, and in the location of her personal property in private spaces."[160] Applying *Karo*, the court found tracking through CSLI likely revealed details about the defendant's home on "several dozen specific occasions," thereby invading his privacy even more than the beeper tracking at issue in *Karo*.[161] Then, applying *Jones*, the court observed that the "privacy interests affected by long-term GPS monitoring . . . apply with equal or greater force to historical CSLI for an extended period of time."[162] Just as the Eleventh Circuit did in *Davis I*, the Fourth Circuit found that cell phones, due to their small size and increasingly inseparable relationship with their users, allow for far more revealing tracking through private and public areas than the tracking of cars.[163]

Expressing concern about the future of location tracking through CSLI, the Fourth Circuit sought to craft a rule that could respond to technological advancements in cellular networks. The court discussed the

---

154 *Id.* at 1217.

155 *Id.* (quoting *In re* Elec. Commc'n Serv. to Disclose, 620 F.3d 304, 317 (3d Cir. 2010) (emphasis in original)).

156 *Id.*

157 *Graham I*, 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

158 *Id.* at 349.

159 *Graham I*, 796 F.3d at 341.

160 *Id.* at 345.

161 *Id.* at 347.

162 *Id.* at 348.

163 *Id.*

rise of small cell technologies, including microcells and femtocells, and "[t]he intense competition among cellular networks" to increase data capacity.[164] Because small cells will likely increase the overall accuracy of CSLI, the court stated that it was obligated to "take such developments into account" when evaluating surveillance through CSLI.[165]

The Fourth Circuit explained at length why the third-party doctrine did not apply to CSLI.[166] The court found that cell phone users do not voluntarily convey CSLI to service providers for several reasons.[167] First, the court observed that a cell phone user "is not required to actively submit any location-identifying information when making a call or sending a message."[168] Instead, the service provider "automatically generates CSLI in response to connections made between the cell phone and the provider's network."[169] Because cell phone users do not actively choose to disclose their information, the court refused to find that users voluntarily disclose their location to their network.[170] According to the court, private information only loses Fourth Amendment protection when it is disclosed consciously and willingly.[171]

Second, the court focused on the important role cell phones play in modern society. The court recognized that "for an increasing portion of our society, [cell phone use] has become essential to full cultural and economic participation."[172] The mere common act of using a cell phone cannot in turn mean that people "have volunteered to forfeit expectations of privacy."[173] Although the court accepted the legitimate business necessity service providers have in generating CSLI, the court feared that application of the third-party doctrine to CSLI would greatly limit the Fourth Amendment in the modern world:

> It turns out that the proliferation of cellular networks has left service providers with a continuing stream of increasingly precise information about the locations and movements of network users. Prior to this development, people generally had no cause for concern that their movements could be tracked to this extent. That new technology has happened to generate and permit retention of this information cannot

164 *Id.* at 350–51.
165 *Id.* at 351.
166 *Id.* at 351–61.
167 *Id.* at 354–56.
168 *Id.* at 355.
169 *Graham I*, 796 F.3d at 354.
170 *Id.*
171 *Id.*
172 *Id.* at 355–56.
173 *Id.* at 356.

> by itself displace our reasonable privacy expectations; nor can it justify inspection of this information by the government in the absence of judicially determined probable cause.[174]

Because of these concerns, the Fourth Circuit refused to expand the third-party doctrine and abrogate a cell phone user's reasonable expectation of privacy in their locational history.[175]

The dissent in *Graham* argued that CSLI should receive no Fourth Amendment protection because it is governed entirely by the third-party doctrine.[176] The dissent argued that cell phone users not only convey CSLI to service providers, but also do so voluntarily.[177] The dissent reasoned that although service providers produce the record of CSLI, it is the user who conveys the underlying data to the service provider by using the phone.[178] Moreover, the user conveys this information voluntarily because all cell phone users know that their phone interacts with the cellular network.[179]

The dissent gave an example from everyday life: "[a]nyone who has stepped outside to 'get a signal,' or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters."[180] According to the dissent, because cell phone users know that their "location matters," they likewise know and accept that a third party has accessed and recorded their location.[181] The dissent acknowledged the temptation of "holding that individuals *always* have a reasonable expectation of privacy in large quantities of location information, even if they have shared that information with a phone company."[182] The dissent concluded, however, that "the third-party doctrine does not afford us that option" because under the doctrine, "the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy."[183]

Although the Ninth Circuit Court of Appeals has yet to decide whether CSLI receives Fourth Amendment protection, several district courts from within that circuit have extended such protection.[184] In 2015, the District

---

174 *Id.* at 359–60.
175 *Id.* at 360–61.
176 *Id.* at 380 (Motz, J., dissenting).
177 *Id.* at 382.
178 *Id.*
179 *Graham I*, 796 F.3d at 382–83.
180 *Id.* at 383.
181 *Id.*
182 *Id.* at 388.
183 *Id.*
184 *See, e.g.*, United States v. Williams, No. 13-CR-00764-WHO-1, 2016 WL 492934,

Court for the Northern District of California in *In re: Application for Telephone Information Needed for a Criminal Investigation*[185] upheld a magistrate order denying the government access to CSLI without obtaining a warrant based on probable cause.[186] Then, on January 7, 2016, in *United States v. Williams*,[187] another judge from the District Court for the Northern District of California held that "defendants had a reasonable expectation of privacy in the CSLI and that probable cause was necessary to obtain [a warrant]."[188]

B. COURTS THAT HAVE HELD THAT THE FOURTH AMENDMENT DOES NOT REQUIRE WARRANTS TO REVIEW CSLI

After the decision in *Davis I*, the Eleventh Circuit agreed to rehear the case en banc.[189] In 2015, in *United States v. Davis* (*Davis II*),[190] the en banc court held that the government's review of the defendant's CSLI did not violate the Fourth Amendment.[191] First, the Eleventh Circuit found that the CSLI related to the defendant's cell phone was a business record owned and generated by his service provider, MetroPCS, in which he could claim no direct interest.[192] Referring to the CSLI as "cell tower records," the court explained that the records "were created by MetroPCS, stored on its own premises, and subject to its control."[193] Therefore, the court found that the service provider had every right to comply with the government's § 2703(d) order and produce its business record of the defendant's location history.[194]

Second, citing *Miller* and *Smith*, the court held that the defendant had neither a subjective nor a reasonable expectation of privacy in the CSLI.[195] Because "cell users know that they must transmit signals to cell towers within range," the court found that they know they are providing location

at *1 (N.D. Cal. Feb. 9, 2016); *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1013 (N.D. Cal. 2015), *appeal dismissed* (Feb. 5, 2016).

185 119 F. Supp. 3d 1011 (N.D. Cal. 2015), *appeal dismissed* (Feb. 5, 2016).

186 *Id.* at 1013.

187 No. 13-CR-00764-WHO-1, 2016 WL 492934 (N.D. Cal. Feb. 9, 2016).

188 *Id.* at *1.

189 United States v. Davis (*Davis II*), 785 F.3d 498, 511 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

190 *Davis II*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

191 *Id.* at 511.

192 *Id.*

193 *Id.*

194 *Id.*

195 *Id.*

information to their service provider, and therefore lack a subjective expectation of privacy.[196] Moreover, the court found that people cannot have a reasonable expectation of privacy in CSLI because *Smith* specifically held that people do not have a reasonable expectation of privacy in the non-content information generated to facilitate phone conversations.[197] Although the Eleventh Circuit recognized that "the landscape of technology has changed" since *Miller* and *Smith*, it was unwilling to depart from such precedent simply because of these technological advances.[198]

After resolving the defendant's challenge through the third-party doctrine, the Eleventh Circuit turned to *Jones*.[199] The Eleventh Circuit feeling the need to distinguish *Jones* noted the two essential differences between the defendant's case and *Jones*: first, in the case before the court, it was a private service provider, not the government, that collected the location information, and second, there was no "physical intrusion on private property" to gather this location information.[200] The court went on, however, to explain "even setting aside the controlling third-party doctrine," CSLI "is materially distinguishable from the precise, real-time GPS tracking in *Jones*," because CSLI cannot "identify the cell phone user's location with pinpoint precision."[201] Because it reveals only the person's general location, the court asserted that CSLI does not pose a serious a threat to privacy.[202] Obviously there are greater privacy expectations when precise information as opposed to general information of one's location is implicated.

The dissent, however, noted that the government obtained sixty-seven days' worth of CSLI, which gave the government access to information related to "5,803 phone calls" or "11,606 data points" on the defendant's location.[203] Therefore, the dissent resisted applying the third-party doctrine to the defendant's claim because allowing the government to obtain such a massive amount of location information without a warrant would greatly diminish the Fourth Amendment's protections in the modern world.[204]

196 *Id.*

197 *Id.*

198 *Id.* at 512.

199 *Id.* at 513.

200 *Davis II*, 785 F.3d at 513.

201 *Id.* at 515.

202 *Id.*

203 *Id.* at 533 (Martin, J. dissenting).

204 *Id.* The dissent gave the example of Google, noting that Google collects not only direct personally identifiable information, such as a user's name, email address, phone number, and credit card information, but also information about a person's Internet habits

Moving past the third-party doctrine, the dissent argued that individuals likely have a reasonable expectation of privacy in CSLI.[205] Observing that "the subjective inquiry is easy," the dissent argued that "people do not expect the government to track them simply as a consequence of owning and using what amounts to a basic necessity of twenty-first century life—the cell phone."[206]

The dissent made note of the rise of small cell technologies to rebut the majority's narrow view of the precision of CSLI.[207] Specifically, the dissent noted that small cells now make it impossible to know how precise CSLI is going to be in a certain case:

> As a person walks around town, particularly a dense, urban environment, her cell phone continuously and without notice to her connects with towers, antennas, microcells, and femtocells that reveal her location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot. And since a text or phone call could come in at any second—without any affirmative act by a cell phone user—a user has no control of the extent of location information she reveals.[208]

According to the dissent, such an unlimited power to gather precise location information about an individual must be fettered by the Fourth Amendment, as an individual should only have such a detailed history of his or her travels reviewed by the government after a judge has found that probable cause justifies this invasion of privacy.[209]

In 2016, in *United States v. Graham* (*Graham II*),[210] the en banc court for the Fourth Circuit Court of Appeals rejected the earlier panel decision and held that the government's review of defendant's CSLI did not violate the Fourth Amendment.[211] The court found that the defendant had voluntarily turned over his location information to his service provider and therefore, under the third-party doctrine, lost any reasonable expectation of privacy in his CSLI.[212] Although the court applied the third-party doctrine,

---

that, when brought together, have the potential to reveal extremely intimate details about a person's life. *Id.* at 535–36. If the third-party doctrine would allow this, then the third-party doctrine must be revised in the light of new technology, for such deeply private information must be protected by the Fourth Amendment. *Id.* at 537.

[205] *Id.* at 538–39.

[206] *Id.*

[207] *Id.* at 541–42.

[208] *Davis II*, 785 F.3d at 541–42.

[209] *Id.* at 542–43.

[210] United States v. Graham (*Graham II*), 624 Fed. App'x. 75 (2015).

[211] United States v. Graham (*Graham III*), No. 12-4659, 2016 WL 3068018 (4th Cir. May 31, 2016).

[212] *Id.* at *1.

it did recognize the uncertain state of law around CSLI, noting how "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case."[213]

The dissent took issue with the majority's conclusion that the defendant had "voluntarily conveyed" his location information at all.[214] "A customer buys a cell phone. She turns it on and puts it in her pocket. With those acts, says the majority, she has 'voluntarily conveyed' an unbounded set of personal location data to her service provider, all of which is unprotected by the Fourth Amendment."[215] The dissent argued that under the third-party doctrine, a defendant conveys information voluntarily only when he has knowledge of the information and takes an affirmative action to transmit that information to a third party.[216] Applying this definition, the dissent explained how "there is no reason to think that a cell phone user is aware of his CSLI, or that he is conveying it."[217] Most cell phone users are completely unaware of the fact that their service provider logs their location not only when they make calls, but also when, as the dissent emphasized, they passively receive calls.[218] Because CSLI is generated without the user's knowledge and often without any accompanying affirmative act, the dissent would have found no voluntary conveyance of information and therefore not applied the third-party doctrine.[219]

In 2016, in *United States v. Carpenter*,[220] the Sixth Circuit Court of Appeals also held that the Fourth Amendment did not require the government to obtain a warrant before reviewing CSLI.[221] The court found that CSLI was not private content, but was instead simply routing information similar to "mailing addresses, phone numbers, and IP addresses" that service providers use to facilitate phone calls.[222] Applying the third-party doctrine, the court relied heavily on *Smith* and found no material difference from the phone numbers collected in *Smith* and the

[213] *Id.* at *2.

[214] *Id.* at *15 (Wynn, J., dissenting).

[215] *Id.*

[216] *Graham III*, 2016 WL 3068018, at *17.

[217] *Id.* at *18.

[218] *Id.* at *18–19.

[219] *Id.* at *18.

[220] United States v. Carpenter, Nos. 14–1572, 14–1805, 2016 WL 1445183 (6th Cir. Apr. 13, 2016).

[221] *Id.* at *1, *5.

[222] *Id.* at *4.

CSLI at issue.[223]

The court stated that CSLI, or at least the CSLI generated given the facts of the case before it, is far less precise than the GPS tracking from *Jones*.[224] The court acknowledged an amicus brief filed by the American Civil Liberties Union, which extensively discussed the rise of small cells in traditional cellular networks.[225] However, the court ignored any concerns regarding small cells, stating that "our task is to decide this case, not hypothetical ones; and in this case there are no femtocells to be found."[226]

The concurrence in *Carpenter* argued that the majority gave short shrift to the defendant's Fourth Amendment concerns.[227] The concurrence argued that by describing CSLI as routing information, the majority failed to capture the privacy interests at stake in CSLI, for mailing addresses, phone numbers, and IP addresses "do not necessarily reflect personal location" in the way CSLI does.[228] The concurrence would have compared CSLI to location information like the GPS data in *Jones*.[229] Although the concurrence accepted that the CSLI at issue in this case was less accurate than the GPS data in *Jones*, it recognized that it may be time "to develop a new test to determine when a warrant may be necessary under these or comparable circumstances."[230]

III. A RIGHT TO BE FREE FROM DRAGNET SURVEILLANCE: THE FOURTH AMENDMENT PROTECTS A PERSON'S CSLI

This Part argues that the government must obtain a warrant before reviewing CSLI.[231] Section A argues that people have a reasonable expectation of privacy in the location information their cell phones generate.[232] Section B explains why the third-party doctrine should not preclude courts from giving CSLI Fourth Amendment protection.[233] Section C asserts that Congress should reform the SCA to mandate probable

---

[223] *Id.* at *5.

[224] *Id.* at *6.

[225] Brief for American Civil Liberties Union et al. as Amici Curiae Supporting Defendants, United States v. Carpenter, Nos. 14–1572, 14–1805, 2016 WL 1445183 (6th Cir. Apr. 13, 2016).

[226] *Carpenter*, 2016 WL 1445183, at *6.

[227] *Carpenter*, 2016 WL 1445183, at *13 (Stranch, J., concurring).

[228] *Id.*

[229] *Id.*

[230] *Id.*

[231] *See infra* notes 252–278 and accompanying text.

[232] *See infra* notes 235–251 and accompanying text.

[233] *See infra* notes 252–268 and accompanying text.

cause warrants for CSLI.[234]

A. PEOPLE POSSESS A REASONABLE EXPECTATION OF PRIVACY IN THEIR LOCATION HISTORY

The U.S. Supreme Court should hold that people have a reasonable expectation of privacy in their location data generated through CSLI, particularly as this location data grows increasingly precise. In finding that cell phone users do not have a reasonable expectation of privacy in CSLI, the Eleventh Circuit in *Davis II* asserted that CSLI "does not identify the cell phone user's location with pinpoint precision."[235] Although this may have been true in a traditional cellular service network composed only of large base stations, in a world of femtocells, picocells, SmartPoles, and other small cell technologies, this is no longer the case.[236] The more precise the information, the greater the chance of pinpointing a user's location. Cell phone users, particularly those that live in dense urban environments, may now generate CSLI that reveals their location to within a matter of feet—not a matter of miles like under the traditional system.[237]

A future where the nearest base station is on the telephone pole outside one's home or inside the hallway of an apartment building is already here in some American cities and will increasingly become the norm based on the projected growth of small cell technologies.[238] Courts must consider CSLI as amplified by small cells in order to truly appreciate the threat to privacy it poses.

Under the distinction the Court formulated in *Knotts* and *Karo*, the government's review of CSLI will often violate a person's reasonable expectation of privacy by revealing information from within a person's home that the government "could not have otherwise obtained without a warrant."[239] Once base stations are immediately outside or even inside a person's home, location information from these stations will perform the

---

[234] *See infra* notes 271–278 and accompanying text.

[235] *Davis II*, 785 F.3d 498, 515 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

[236] *See supra* notes 49–70 and accompanying text (discussing the rise of small cell technologies).

[237] *See* Brief for American Civil Liberties Union et al. as Amici Curiae Supporting Defendants, United States v. Carpenter, Nos. 14–1572, 14–1805, 2016 WL 1445183 (6th Cir. Apr. 13, 2016), 14–20.

[238] *See, e.g.*, DeGrasse, *supra* note 66 (describing Verizon's planned installation of 400 small cells on light poles and utility poles in San Francisco); Soder, *supra* note 61 (outlining Verizon's plans for installing small cells on street lights and utility poles in Cleveland); Tilley, *supra* note 67 (discussing the installation of SmartPoles in Los Angeles).

[239] United States v. Karo, 468 U.S. 705, 715 (1984).

same function that the concealed beeper did in *Karo*.[240] CSLI will be able to tell the government "that a particular article," in this case a person's cell phone, "is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched."[241] This is beyond the mere augmentation of regular police surveillance permitted in *Knotts*; this is the "dragnet-type law enforcement practices" of "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision" of which the *Knotts* Court warned.[242] Warrantless collection of CSLI would allow the government to track people after they have retreated into their homes, the area granted the greatest privacy protections under the Fourth Amendment.

Looking beyond CSLI collected from within a person's home, the government's review of CSLI also violates one's reasonable expectation of privacy under the analysis endorsed by the five Justices in *Jones*.[243] Although Justice Alito could not draw a precise line as to when location monitoring through advanced technology violated a person's reasonable expectation of privacy, he accepted that at a minimum, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy" because people do not reasonably expect their whereabouts to be monitored for an extended period of time by law enforcement.[244] The GPS monitoring in *Jones* took place over twenty-eight days.[245] The CSLI monitoring in *Davis II* took place over sixty-seven days, generating 11,606 data points tracing the defendant's location,[246] while the CSLI monitoring in *Graham* took place over 221 days.[247] It would be shocking if the CSLI monitoring at issue in both of these cases failed to meet the standard of long-term location monitoring that violates a person's reasonable expectation of privacy.

Moreover, even shorter-term monitoring may violate the theory of

---

240 *See id.*

241 *Id.*

242 United States v. Knotts, 460 U.S. 276, 284 (1983).

243 *See* United States v. Jones, 132 S. Ct. 945, 954–55 (2012) (Sotomayor, J., concurring) (accepting that long-term GPS monitoring would violate a person's reasonable expectation of privacy); *id.* at 964 (Alito, J., concurring in the judgment) (stating that GPS surveillance of longer than four weeks violates a person's reasonable expectation of privacy).

244 *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

245 *Id.* at 948.

246 *Davis II*, 785 F.3d 498, 533 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

247 *Graham I*, 796 F.3d 332, 341 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

reasonable expectation of privacy advanced by Justice Sotomayor in *Jones*.[248] According to Justice Sotomayor, all location tracking through advanced technology granted the government the power to amass "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[249] Even a relatively short period of location monitoring through CSLI could reveal a wide array of deeply personal and private information. The continuous and precise monitoring presents serious issues as to whether we as a free society should accept this intrusion by the government. Likewise, Justice Alito in his *Jones* concurrence struggled to draw an exact line between long- and short-term monitoring, a problem that has plagued the appellate courts confronting CSLI tracking as well.[250] Therefore, in order to craft a rule that gives the government proper notice as to what actions will and will not violate the Fourth Amendment, the Court should hold that people have a reasonable expectation of privacy in all CSLI, regardless of the amount collected by the government.

By focusing on CSLI generated from traditional cellular networks, the Eleventh Circuit in *Davis II* drastically underestimated the precision of CSLI.[251] A court that confronts tracking through CSLI must take into account the rise of small cell technologies. And when such a court considers a future where every street lamp could be a cell tower and every apartment, office, or public park comes equipped with its own dedicated team of femtocells and picocells, it must find that, despite these technological encroachments, people retain a reasonable expectation of privacy in their movements through the day.

B. THE THIRD-PARTY DOCTRINE DOES NOT PRECLUDE PROTECTION

Having established that people have a reasonable expectation of privacy in their CSLI, the third-party doctrine does not apply to CSLI because cell phone users do not "voluntarily convey" their location to their service providers. In both *Miller* and *Smith*, the defendants made an active

---

[248] *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

[249] *Id.* at 955.

[250] *Id.* at 964 (Alito, J., concurring in the judgment); *Graham I*, 796 F.3d at 350 (holding that "the government engages in a Fourth Amendment search when it seeks to examine historical CSLI pertaining to an extended time period like 14 or 221 days"); *Davis II*, 785 F.3d at 516 (stating that CSLI of a period of 67 days did not reveal "anything close to [an] 'intimate portrait' of [the defendant's] life").

[251] *Davis II*, 785 F.3d at 515 ("Historical cell tower location data does not identify the cell phone user's location with pinpoint precision . . . .").

choice to give certain information to a third party.[252] By writing checks and making deposits, the defendant in *Miller* created the financial documents at issue and voluntarily conveyed them to the bank.[253] By manually punching numbers into his telephone, the defendant in *Smith* actively provided the phone company with the exact same information later used against him in a criminal trial.[254]

Unlike *Miller* and *Smith*, service providers passively collect CSLI each time a user's phone connects to a base station. As the Fourth Circuit Court of Appeals recognized in *Graham I*, a cell phone user "is not required to actively submit any location-identifying information when making a call or sending a message."[255] Rather, the information at issue is information that the service provider "automatically generates . . . in response to connections made between the cell phone and the provider's network."[256] Although CSLI is generated when cell phone users make the active choice to place a phone call, CSLI is also generated when users make no active choice at all, such as when they receive calls or text messages or, for smartphone users, when applications connect to the network for updates.[257] It is difficult to see how users voluntarily convey anything when they receive unsolicited calls from telemarketers or when applications built into their phone silently update in the background.

The Eleventh Circuit Court of Appeals in *Davis II* incorrectly equated a cell phone user's vague awareness of how a cell phone functions with the active choices the defendants made in *Smith* and *Miller*.[258] In *Smith*, the Court could draw a clear line from the defendant's choice to give telephone numbers to the phone company and the government's later use of those phone numbers as evidence.[259] With the conveyance of CSLI, the line is far less clear, as no service provider requires its users to manually enter their location each time they place a call.[260]

Even if the U.S. Supreme Court were to find that cell phone users voluntarily convey their location information to their service providers, the

---

[252] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

[253] *See Miller*, 425 U.S. at 438, 442.

[254] *Smith*, 442 U.S. at 742–43.

[255] *Graham I*, 796 F.3d 332, 355 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

[256] *Id.* at 354.

[257] *See id.* at 355.

[258] *Davis II*, 785 F.3d 498, 511–12 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

[259] *Smith*, 442 U.S. at 742–44.

[260] *Graham I*, 796 F.3d at 355.

Court should take up the questions Justice Sotomayor raised in *Jones* and reexamine the continued viability of the third-party doctrine in the digital age.[261] The observations made by the Eleventh Circuit in *Davis II* and the dissent in *Graham I* are not without merit. As the dissent in *Graham I* observed, on some level, cell phone users who run outside when they receive an important call do understand that in order to get a better signal "location matters."[262] However, if the third-party doctrine allows the government unfettered access to location data on all Americans who—at even the most archaic level—understand that their information is accessible to any company that provides a digital service, then as the dissent in *Davis II* observed, the Fourth Amendment offers shrinking protection in the increasing online world.[263] Justice Sotomayor explained in her concurrence in *Jones* that in order to participate in modern society, people must disclose all sorts of private information, whether through accessing emails, shopping online, or carrying a cell phone.[264] Further, in *Riley v. California*, the Court unanimously recognized the essential role cell phones have in the modern world.[265]

The Court confronted a similar doctrinal challenge in *Katz*. In *Katz*, rigid application of the Fourth Amendment's trespass theory—the only theory that existed at the time for showing a constitutional violation—would have granted the government the power to listen in on the defendant's private conversation.[266] The Court refused to allow old doctrines to interfere with the core privacy protections of the Fourth Amendment.[267] Instead, the Court formulated a new approach that properly considered "the vital role that the public telephone has come to play in private communication."[268] Similarly, in *Riley v. California*, the Court

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

[262] *Graham I*, 796 F.3d 332, 383 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). (Motz, J., dissenting).

[263] *Davis II*, 785 F.3d at 537 (Martin, J., dissenting) (discussing the problems that "result from a wooden application of the third-party doctrine" in the digital age).

[264] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[265] Riley v. California, 134 S. Ct. 2473, 2484 (2014) (observing that cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

[266] Katz v. United States, 389 U.S. 347, 351 (1967).

[267] *Id.* ("But this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this. For the Fourth Amendment protects people, not places") (internal citations omitted).

[268] *Id.* at 352.

adopted a new doctrine to deal with searches incident to an arrest when the search involves a cell phone.[269]

Today's Supreme Court faces an equally important choice. If the Court finds that the third-party doctrine stands in the way of protecting CSLI from warrantless searches, then the Court must refashion its old doctrine. Whether the Court finds that passive collection is different than active disclosures, or whether it simply decides that the doctrine as a whole must be discarded in the digital realm, it must not stand by and allow the third-party doctrine to swallow the Fourth Amendment.

C. BRINGING THE SCA INTO THE 21ST CENTURY

Congress should also acknowledge the radical technological changes that have occurred over the past thirty years and remove § 2703(d) orders from the SCA. When the SCA was enacted, Congress could not possibly have envisioned a future where cell phones were omnipresent and inseparable from their users. Requiring only "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation" for a court order for CSLI[270] may have made sense when the United States had only 1,531 cell sites, as it did in 1994.[271] It does not make sense today in a country that contains millions of cell sites, through which the government can gain access to a person's movements within ten-foot increments through the use of small cells.

In order to best protect location privacy in the modern world, Congress must require prosecutors to go before a judge and make a showing of probable cause before obtaining access to this trove of location information. Because small cell technologies are evolving so rapidly, Congress may be better suited than the courts to respond to these developments. Congress should follow Justice Alito's instruction from his concurrences in *Jones* and *Riley* and craft comprehensive legislation that balances the competing interests at stake in these cases.[272]

---

[269] Riley v. California, 134 S. Ct. at 2494–95.

[270] 18 U.S.C. § 2703(d) (2012).

[271] Brian L. Owsley, The Honorable, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 33 (2013-2014).

[272] Riley v. California, 134 S. Ct. at 2497–98 (Alito, J., concurring in part and concurring in the judgment) (noting that "after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners," legislatures should be free to "enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables. . . . Legislatures, elected by the people, are in a better position than

In doing so, Congress must follow the Fourth Amendment requirements of probable cause and particularity and demand that orders for CSLI only issue upon probable cause and are only directed at particularized targets whose accounts contain evidence of the crime under investigation. The lower § 2703(d) standard follows from the reasonable suspicion standard the U.S. Supreme Court formulated in *Terry v. Ohio*.[273] The Court in *Terry*, however, permitted this lower justification only because the intrusion at issue—a pat-down—was minor; an officer "for the protection of himself and others" was permitted only "to conduct a carefully limited search of the outer clothing" of the target.[274] When the government reviews CSLI, it gains access to the precise details of a person's movements across a potentially vast period of time. This is far beyond the "carefully limited search" the *Terry* standard authorized. Because the government's review of CSLI represents a large intrusion into the precise details of a person's movements, the government must in turn justify its search under a more stringent standard.

Congress must reform both components of the § 2703(d) standard. First, it must require a showing of probable cause, not reasonable suspicion, to obtain access to CSLI. Reasonable suspicion demands too little from the government, as courts have routinely recognized the low showing needed to meet the reasonable suspicion burden. Under a probable cause standard, the government will have to present "reasonably trustworthy information . . . to warrant a man of reasonable caution in the belief that an offense has been or is being committed."[275] A probable cause standard will thereby ensure that the government gathers CSLI only when it suspects a person of committing a crime, rather than merely having information "relevant and material" to an investigation.[276] In this way, a probable cause standard gives proper protection to the sensitive information of the general public, while still

we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."); United States v. Jones, 132 S. Ct. at 945, 964 (2012) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.").

[273] Terry v. Ohio, 392 U.S. 1, 30 (1968).

[274] *Id.*

[275] Brinegar v. United States, 388 U.S. 160, 175–76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1924)).

[276] *See* Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1902–03 (2011) ("Compared to probable cause, disclosure under the relevant and material standard is both lower in the quantum of evidence required and broader in the individuals it can potentially target, particularly third parties.").

allowing the government to target suspected criminals.

Second, Congress—cognizant of the Fourth Amendment's particularity requirement—should allow orders for CSLI to issue only when the government has shown that the order will reveal evidence of a crime. By allowing the government to access CSLI if it is "relevant and material" to its investigation, § 2703(d) allows the government access to the CSLI of too many innocent people who may have only a tangential connection to a criminal investigation. The Fourth Amendment was designed to prevent legislatures from issuing general warrants that would grant government agents the power to search and seize whatever and whomever they so choose.[277] In order to ensure that application for such orders for CSLI do not authorize dragnet surveillance of an unknown number of people, Congress must demand that the government explain how the CSLI sought will reveal evidence of a crime.[278]

CONCLUSION

From femtocells in our homes to picocells on our streetlamps, small cell technologies are spreading rapidly across the United States. Although small cells will provide many benefits to consumers, they have the chance to seriously erode privacy. The Stored Communications Act allows the government to obtain historical cell site location information without a Fourth Amendment warrant. Small cells will make CSLI increasingly precise, allowing the government to chart a person's movements down to a matter of feet. When deciding whether CSLI receives Fourth Amendment protection, courts must consider the cellular network of the near future, where most towers are no longer massive antennas, but are instead no larger than a breadbox. Therefore, courts should hold that the Fourth Amendment requires the government to obtain a particularized warrant supported by probable cause before it can review CSLI. Moreover, Congress should recognize the increased privacy interests people have in CSLI and reform the SCA to require a higher showing for court orders for CSLI. At its core, the Fourth Amendment must prevent the government from tracking its citizens from morning to night, through commute, work, church, and home, for days on end, without first obtaining a particularized warrant supported by probable cause. The rise of small cells cannot deprive the people of this fundamental guarantee.

---

[277] *Brinegar*, 338 U.S. at 176 ("To allow less [than probable cause] would be to leave law-abiding citizens at the mercy of the officers' whim or caprice.").

[278] Freiwald, *supra* note 15, at 696–98.

"Only time will tell whether our society will prove capable of preserving age-old privacy protections in this increasingly networked era."[279]

[279] *Graham III*, No. 12-4659, 2016 WL 3068018 at *1, *23 (4th Cir. May 31, 2016) (Wynn, J., dissenting).