University of Miami Law Review

Volume 70
Number 4 *Volume 70 Number 4 (Summer 2016)*

Article 9

8-1-2016

Cellphones, Stingrays, and Searches! An Inquiry into the Legality of Cellular Location Information

Jeremy H. D'Amico

Cellphones, Stingrays, and Searches! An Inquiry into the Legality of Cellular Location Information

JEREMY H. D'AMICO*

Can the Fourth Amendment protect an individual's right privacy by preventing the disclosure of her location through cell site location information? Does it currently? Should it? Many court opinions answer these questions in both the affirmative and the negative. The rationale underlying each conclusion is disparate. Some rely on statutory regimes, others rely on the United States Supreme Court's interpretation of reasonableness. However, Cell Site Location Information is a technology that requires uniformity in its interpretation. This note investigates the different interpretations of the Fourth Amendment as it relates to Cell Site Location Information. It explains the technology behind Cell Site Location Information, and then proffers a framework to unify the analysis of whether there is an expectation in Cell Site Location Information by modifying the U.S. Supreme Court's Katz test. This note does not seek to offer an opinion on whether Cell Site Location Information should be within the zone of reasonable privacy expectations. Instead, the analytical framework internalizes the privacy interests of the individual and the governmental interest in ferreting out crime. It is striking this balance when analyzing these issues that

* J.D. Candidate 2015, University of Miami School of Law. I thank Brian S. Goldenberg for his inspiration, the members of the University of Miami Law Review, and the University of Miami School of Law.

will help the courts to uniformly investigate the privacy implications of Cell Site Location Information.

INTRODUCTION

In 1973, Martin Cooper placed the first public cellphone call from Manhattan.[1] Today, cellphones are remarkably small and have more computational capacity than NASA had during the Apollo

[1] *Mobile phone's 40th anniversary: from 'bricks' to clicks*, THE GUARDIAN (Apr. 3, 2013, 3:05 PM), http://www.theguardian.com/technology/2013/apr/03/mobile-phone-40th-anniversary.

era.[2] Cellphones are no longer used solely to place phone calls, making the term almost a misnomer. Chief Justice Roberts aptly noted that cellphones can "easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[3] Many people rely on their cellphones daily, such that the "proverbial visitor from Mars might conclude they were an important feature of human anatomy."[4] A cellphone can now perform a number of tasks: make calls, send texts and e-mails, run apps, and explore the internet. But, the way a cellphone enables the performance of those tasks may remove any expectation of privacy not just of its contents but also in the user's location. Depending on the jurisdiction, the government can obtain location information without a warrant or probable cause, so long as it can show that the location information is relevant to any ongoing criminal investigation—even one that is not targeting the user.

The benefits of a modern cellphone that contribute to its ubiquity come with a burden: law enforcement agencies can acquire a person's cell-site location information ("CSLI") cheaply and quickly, and they can do so without ever contacting the user.[5] Considering that most adults carry a cellphone,[6] a broad interpretation of the third-party doctrine has allowed government actors to track a person's movements while evading the strict statutory requirements for affixing a tangible tracking device to one's property.

The application of the third-party doctrine has led to conflict among state supreme courts, federal courts of appeals, and several lower courts. As a result, courts have drawn unworkable distinctions. For instance, courts disagree not only on the ultimate issue of whether obtaining CSLI without a warrant is a search, but they also

---

[2] *Do-It-Yourself Podcast: Rocket Evolution*, NASA, http://www.nasa.gov/audience/foreducators/diypodcast/rocket-evolution-index-diy.html (last visited Oct. 26, 2015) (noting that a "cell phone has more computing power than the computers used during the Apollo era").

[3] Riley v. California, 134 S. Ct. 2473, 2489 (2014) (holding a warrantless search of the contents of a cellphone absent exigent circumstances unconstitutional under the Fourth Amendment).

[4] *Id.* at 2484.

[5] *See* 18 U.S.C. § 2703 (2012); *see also infra* Section III.C.

[6] *See* Lee Rainie, *Cell phone ownership hits 91% of adults*, PEW RESEARCH CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

disagree about the legal mechanism that empowers the government to obtain CSLI. This debate has provided fertile ground for many notes, comments, and scholarly articles.[7] In addition, the recent outing of law enforcement's use of Stingray devices,[8] or "portable personal cell towers," adds yet another element to the inquiry. These Stingray devices simulate third-party service providers and function under the umbrella of cellular technology. Because Stingray systems do not require a third-party service provider, the constitutionality of their use may pose related but different questions regarding their legality.

Can the protection offered by the Fourth Amendment continue perpetually in the face of these technologies? This comment surveys the CSLI debate. Part II lends a much-needed survey of the technology behind CSLI and Stingray devices. Part III summarizes the current state of privacy jurisprudence. Part IV discusses the argument surrounding whether obtaining CSLI is an unreasonable search. Part V tackles the privacy implications regarding the government's use of Stingray technology. Last, although a litany of scholarship surrounds the CSLI debate, many advocate for a legislative solution. However, notwithstanding the calls for congressional reform, there have been few other solutions suggested. Thus, Part VI propounds an analytical framework that adequately balances private and governmental interests in the digital age—at least when cellular location information is involved.

I. THE TECHNOLOGY: CELLPHONES, CELL SITES, AND CELL-SITE LOCATION INFORMATION

Undoubtedly, cellphones changed the way people communicate by telephone.[9] Prior to cellphone use, a person would call a home or office with the hope that the recipient was at the place called. Now, as Matthew Blaze, a Professor of Computer and Information Science

---

[7] *See* discussion *infra* Parts III, IV, and V.

[8] Brad Heath, *Police secretly track cellphones to solve routine crimes*, USA TODAY (Aug. 24, 2015), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[9] *See* PAUL BEDELL, CELLULAR NETWORKS: DESIGN AND OPERATION—A REAL WORLD PERSPECTIVE 14 (2014) [hereinafter BEDELL, CELLULAR NETWORKS]; *see also infra* Part III.

at the University of Pennsylvania, puts it, "Rather than thinking about the telephone located in a place that we call, we think about the person we want to call, because we expect them to have their telephone with them."[10] CSLI is the mechanism that allows a cellphone to function through a network.[11] Like other technologies, the technology pertaining to cell-site location information has become increasingly more accurate over time. As discussed below, CSLI is now able to locate a person within a single room.[12] When a call is placed or when a text message is sent or received, incidental data is also transmitted between a cellphone and the service provider's cell site.[13] It is vital to the privacy debate to fully understand CSLI. Without understanding how a cellphone transmits its location, any analysis of reasonable expectations of privacy in CSLI is fruitless.

A. *Cellphone-to-Cell-Tower Communication*

While travelling on an intestate, most of us have seen a cell tower or cell site.[14] Cell sites appear either as large metal towers in plain view or as poorly disguised trees that dwarf the natural trees

---

[10] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 13 (2010) [hereinafter *June 2010 Hearing*] (testimony of Matt Blaze, Associate Professor, University of Pennsylvania), http://judiciary.house.gov/_fileshearings/printers/111th/111-109_57082.PDF.

[11] For an in-depth discussion of cellular communications, see, for example, PAUL BEDELL, WIRELESS CRASH COURSE—A REAL WORLD PERSPECTIVE (3d ed. 2012) [hereinafter BEDELL, WIRELESS]. *See also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702–16 (2011) (discussing the breadth and richness of information that cellphones communicate to cell towers).

[12] *June 2010 Hearing*, *supra* note 10, at 16.

[13] *See* Tracey v. State, 152 So. 3d 504, 507 n.1 (Fla. 2014) (explaining that CSLI is created when a placed call is received). Location information is also given off by a cellphone passively. *See* Thomas Farley & Ken Schmidt, *Cellular Telephone Basics*, PRIVATELINE (Jan. 1, 2006), www.privateline.com/mt_cellbasics/iii_cell_sector_terminology/.

[14] *See* En Banc Brief of the United States of America at 8, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) [hereinafter Brief of the United States] (en banc). A "Cell Site" is the source of the signal that a cellphone receives, enabling the phone to send and receive calls and data. *See* Farley & Schmidt, *supra* note 13.

that surround it.[15] Alternatively, in urban settings, such as Miami, cell sites are generally located on tall buildings.[16] Cell sites are aptly named because each tower is a site that emanates cellular-signal coverage to a corresponding "cell."[17] It may help to think of the cell site as the dot in the center of a circle with the cell being the circumference of the geographic area that the circle covers.[18]

The size of a cell depends on "terrain, system capacity needs, and geographic location—urban or rural."[19] Size also depends on the number of users attempting to send or receive data b ecause each cell site has a limited amount of information it can transmit between users at one time.[20] For example, a person who attempts to make a call at midnight on New Year's Eve has likely experienced this phenomenon, where the phone struggles to connect a call.[21] This problem is prevalent in populous areas. Thus, the large population in urban areas requires cell sizes to be much smaller and more numerous to accommodate increased cellular-data traffic.[22] This means that the area in which a cellphone will connect to a particular cell tower is smaller. The coverage of cell sites are "shrinking rapidly" because

---

[15] BEDELL, WIRELESS, *supra* note 11, at 14–15.

[16] *Id.* at 21.

[17] A "cell" is the area of coverage that a cell tower provides. *See* Farley & Schmidt, *supra* note 13.

[18] A more accepted depiction of a "cell" is that of a triangle or hexagon because if circles are amassed there would gaps in coverage at the edges whereas triangles or hexagons may be neatly placed next to one another without gaps in coverage, which allows for call hand-off between cells. This shape is also preferred because of the use of sectoring. For a graphic illustration, see Farley & Schmidt, *supra* note 13.

[19] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 10.

[20] *Id.* at 28–32.

[21] *See id.* at 10 ("[A]s data becomes more of a driver of site capacity, additional sites are required to support the capacity needs of the network . . . reduc[ing] the coverage area of the sites while adding more sites to the network."); *see also* BEDELL, WIRELESS, *supra* note 11, at 11–13.

[22] *See* BEDELL, CELLULAR NETWORKS, *supra* note 10, at 22 (stating that microcells have a cell radius of less than 1.3 miles and that picocells have a radius of only 200 meters); *see also* BEDELL, WIRELESS, *supra* note 11, at 27–29 (discussing the difference in range between macro-, micro-, and pico-cells).

of these high traffic demands, thus making CSLI data more precise in virtually all environments.[23]

One method used by service providers to accommodate increased traffic demands is called "sectoring" or "sectorization."[24] "In today's wireless networks, all cell [sites] are sectorized," which allows customers to reap enhanced coverage benefits.[25] Sectoring breaks one cell site into many cell sites through the use of directional antennas.[26] Again, imagine a cell site as a dot in the center of a circle. Now, imagine that the circle is broken into three or six slices (like a pizza). If a cell tower has three sectors, each sector covers a 120-degree slice of the 360-degree circle; if it is broken into six sectors, then each sector covers 60 degrees of the circle. Each slice is a "sector" that operates under its own frequency and transmits information only to and from cellphones within its sector.[27] Thus, using its records, a cellphone company can determine the sector within which a cellphone is located, making location information in sectorized cells more accurate.[28]

In addition to smaller cell size and sectoring, service providers created networks of overlapping cell sites to ensure consistent coverage for its users.[29] Overlapping cells allow a device to receive a "usable signal" easily as the user moves from one cell site to the

---

[23] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 14; *see also* En Banc Brief of Amicus Curiae AT&T Mobility, LCC in Support of Neither Party at 9, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) [hereinafter Brief of AT&T] (en banc) ("As the density of the cell towers increases . . . the precision of the CSLI increases correspondingly.").

[24] BEDELL, WIRELESS, *supra* note 11, at 113–16.

[25] *Id.* at 116 (discussing the benefits of sectoring as minimizing interference and increasing capacity of a coverage area).

[26] *Id.* at 113–16.

[27] *See* BEDELL, CELLULAR NETWORKS, *supra* note 9, at 90 (stating each sector operates under its own set of frequencies or channels); *see also June 2010 Hearing*, *supra* note 10, at 24 (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier.").

[28] *June 2010 Hearing*, *supra* note 10, at 26 (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("[I]t has become practical for a network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.").

[29] *See* BEDELL, CELLULAR NETWORKS, *supra* note 9, at 30 (discussing the design of cellular networks).

next.[30] If this were not the case, then each time a user exited a coverage cell, the call would drop. A cellphone automatically transitions from cell site to cell site by passively "monitor[ing] its signal levels, and determin[ing] how and when to hand off its transmission to an adjacent cell."[31] This "handing off" also occurs among sectors within a cell site as the cellphone attempts to maintain the strongest signal.[32] Thus, overlapping cell sites allow a service provider to ascertain the path a cell user took by looking to the cell sites and sectors the phone transitioned between along a route.

Cell sites must know where each cellphone is located so that information can be transmitted directly to that device and no other device. This communication between a cell site and cellphone occurs because each cellphone has a unique identifier that allows a cell site to locate and direct information to that particular cellphone.[33] Moreover, cellphones constantly communicate with cell sites through a process known as "registration."[34] Registration is the process the cellphone undergoes for "call handoff" whereby the cellphone monitors its signal strength and switches to the cell site with the strongest connection, and it can occur "every seven seconds."[35] Its purpose is to make sure that the cell network properly routes a call or text message when the user receives or sends one.[36] This self-monitoring of

---

[30] BEDELL, WIRELESS, *supra* note 11, at 40.

[31] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 32; *see also June 2010 Hearing*, *supra* note 10, at 13 (testimony of Matt Blaze, Associate Professor, University of Pennsylvania) (stating that as cellphones move, they "discover the [cell site] with the strongest radio signal and perform a registration process identifying themselves . . . [and] establishing that the user has a valid cell phone service").

[32] *See* BEDELL, CELLULAR NETWORKS, *supra* note 9, at 91 (describing each sector as having its own coverage area within the cell).

[33] *See generally* U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), http://www.justice.gov/opa/file/767321/download [hereinafter USE OF CELL-SITE SIMULATOR TECHNOLOGY].

[34] *See June 2010 Hearing*, *supra* note 10, at 14 (testimony of Matt Blaze, Associate Professor, University of Pennsylvania) (stating that without registration data, the cell-service provider "won't know how to get calls to you").

[35] *See In re* U.S. for Order Directing a Provider of Elec. Commc'n, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (noting that registration "occurs approximately every seven seconds"), *vacated*, 620 F.3d 304 (3d Cir. 2010); *see also* Farley & Schmidt, *supra* note 13.

[36] *See* Farley & Schmidt, *supra* note 13.

signal strength allows the user to continuously have reception, make or receive calls, and use data—all without requiring the user to be involved in the process. In effect, self-monitoring creates many points at which the phone's location can be ascertained.[37]

In recent years, cellphones became "smartphones" and many users now access the internet with their cellphones.[38] The implications of this use on location information are also important to the CSLI debate. As the demand for cellphones with internet connectivity increases, the supply of cell sites that can accommodate this use also increases.[39] By directing more data transmission to each individual cellphone, cell sites can accommodate fewer devices. To solve this issue, service providers have increasingly relied on the use of "microcells," "picocells," and "femtocells" to increase the amount of data that can be processed in a particular area, which allows a cellphone to send and receive more information.[40] These systems are increasingly employed in highly populated areas such as cities, train stations, and airports.[41] Microcells, initially used as "gap fillers" to extend coverage to the small areas between larger cell sites,[42] are now employed with greater frequency to accommodate the increased demand for internet service.[43] Picocells are designed to accommodate smaller areas such as train stations, planes, and office

---

[37] *See* Brief of AT&T, *supra* note 23, at 8 ("At the most basic level, the wireless network needs to determine the location of the mobile device in order to send and receive communications to and from that device."); *see also id.* at 9 (explaining that CSLI is created from voice, text, e-mail, and other data transmissions).

[38] *Wireless Quick Facts*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last visited Apr. 9, 2016) ("Smartphones comprise 77% of traffic on wireless networks . . . .").

[39] *See* 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; *see also Annual Wireless Industry Survey*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last updated June 2015) (data reveals that cell-data usage in America more than doubled between 2012 and 2014).

[40] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 10.

[41] BEDELL, WIRELESS, *supra* note 11, at 27–32.

[42] *Id.* at 28 ("Microcell[s] . . . can be used to add capacity . . . where there is evidence of a very high volume of network traffic.").

[43] *Id.*

buildings.[44] Picocells have a range of less than 200 meters.[45] Femtocells are used to provide cell service to homes and small businesses.[46] Femtocells have a range of less than ten meters.[47] Further, Picocells and Femtocells are designed to bring cell service indoors;[48] therefore, in some instances, they provide cell-site location information where GPS location information would be unavailable because satellite signals cannot communicate to the cellphone's antenna when the signal is blocked.[49] Location information derived from these systems can provide information that is accurate within thirty feet of a person's location.[50]

Not only is cell-site location information becoming precise, but also many service providers store CSLI for business purposes in the form of call records.[51] Call records include the "identity of the cell sector that handled" the call and "may include even more detailed information such as registration data or the cellular telephone user's latitude and longitude."[52] Although each provider has its own retention policies, many providers store "call detail records," which may

---

[44] *Id.* at 29.

[45] *Id.*; *see* BEDELL, CELLULAR NETWORKS, *supra* note 9, at 23.

[46] BEDELL, WIRELESS, *supra* note 11, at 30.

[47] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 24.

[48] BEDELL, WIRELESS, *supra* note 11, at 27–32.

[49] *Id.* at 27–29.

[50] BEDELL, CELLULAR NETWORKS, *supra* note 9, at 24; *see also Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and erance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 33 (2013) [hereinafter *April 2013 Hearing*] (statement of Catherine Crump, Staff Attorney, American Civil Liberties Union) ("[C]ellular towers now may cover an area as small as a tunnel, a subway, a specific roadway, a particular floor of a building, or even an individual home or office.").

[51] Steven Nelson, *Here's How Long Cellphone Companies Store Your Call Records*, U.S. NEWS (May 22, 2015, 2:00 PM), http://www.usnews.com/news/articles/2015/05/22/how-long-cellphone-companies-store-your-call-records (stating that service providers store call records between zero and ten years depending on the provider).

[52] Commonwealth v. Augustine, 4 N.E.3d 846, 854 n.19 (Mass. 2014) (citing *April 2013 Hearing*, *supra* note 50, at 57 (statement of Matt Blaze, Professor, University of Pennsylvania).

"include the most accurate location information available to them" and might even encompass the latitude and longitude of the phone.[53]

Cellphone users now stream music and movies, make calls, send photos and e-mails, check the weather, get directions, and upload data. Performing these activities have forced cell sites to shrink. CSLI is more precise and more revealing of intimate details of one's daily activities than ever before.[54] With this understanding of the technology behind CSLI, an inquiry into privacy expectations can now be had.

II. THE CURRENT STATE OF AFFAIRS: PRIVACY EXPECTATIONS, THE THIRD-PARTY DOCTRINE, AND STATUTES

A. *Privacy Expectations*

Privacy expectations under the Fourth Amendment evolve with society.[55] Originally, a "search" occurred only if the government

---

[53] *April 2013 Hearing*, *supra* note 50, at 57 (statement of Matt Blaze, Professor, University of Pennsylvania).

[54] *See June 2010 Hearing*, *supra* note 10, at 16 (testimony of Matt Blaze, Associate Professor, University of Pennsylvania) (noting that "as we have moved toward very small sector locations," it has become easier to determine a cellphone user's exact location); *see also Annual Wireless Industry Survey*, *supra* note 39 (revealing that cell-data usage in America more than doubled between 2012 and 2014).

[55] For a thoughtful history of the circumstances surrounding the evolution of the Fourth Amendment, see Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 257 (2016) ("By design, therefore, a paramount purpose of the Fourth Amendment was to serve as a guardian of individual liberty and free expression."). A few cases decided by the Supreme Court illustrate this point. *See* Boyd v. United States, 116 U.S. 616 (1886) (holding that compelling a man to produce his papers was a search under the Fourth Amendment), *overruled by* Warden v. Hayden, 387 U.S. 294 (1967); Olmstead v. United States, 277 U.S. 438, 465 (1928) ("The language of the [Fourth A]mendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967) (expanding protections beyond trespass to constitutionally protected areas and including reasonable expectations of privacy); Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013) ("The *Katz* reason-

trespassed on a constitutionally protected area: "persons," "houses," "papers," and "effects."[56] Generally, it appears that the Supreme Court had little difficulty distinguishing private matters within the home from public matters outside of the home.[57] But, in 1967, the Supreme Court blurred this distinction by protecting privacy rights beyond constitutionally enumerated areas.[58] In *Katz v. United States*, the Supreme Court uprooted the classic trespass theory of Fourth Amendment protections by extending Fourth Amendment protection to "people, not places."[59] From then on, a person's Fourth Amendment rights would no longer rely solely on trespass theory. Instead, these protections would be assessed both under trespass theory and by a person's reasonable expectation of privacy beyond constitutionally protected areas.[60]

---

able-expectations test 'has been *added to*, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment . . . ." (quoting United States v. Jones, 132 S. Ct. 945, 952 (2012))).

[56] *See Olmstead*, 277 U.S. at 466 (holding that a person has no reasonable expectation of privacy in communications that are heard beyond the walls of one's home when the government uses a wiretap); *see also* U.S. CONST. amend. IV ("The 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.").

[57] *See, e.g.*, *Olmstead*, 277 U.S. 438; Goldman v. United States, 316 U.S. 129, 134 (1942) (holding that use of a "detectaphone" placed against an adjoining wall to hear conversations on the other side did not constitute a search), *overruled in part by Katz*, 389 U.S. at 353; Silverman v. United States, 365 U.S. 505, 507 (1961) (holding a search unconstitutional when government affixed a "spike mic" to apartment's heating conduit, allowing them to eavesdrop on conversations); *id.* at 509–10 (noting that "[e]avesdropping accomplished by means of such a physical intrusion" violated the Fourth Amendment); Berger v. New York, 388 U.S. 41, 59 (1967) (striking down a New York wiretapping statute and stating that "[d]uring such a long and continuous (24 hours a day) period the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation").

[58] *See generally Katz*, 389 U.S. 347.

[59] *Id.* at 351.

[60] *Id.* at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and,

Since *Katz*, the Supreme Court has articulated some guidance on what is a reasonable expectation of privacy.[61] A person has no reasonable expectation of privacy on public roads.[62] Nor is there a reasonable expectation of privacy in open fields.[63] Nor does a person have a reasonable expectation of privacy when technology in "general public use" reveals intimacies of his home.[64] But, whether a person maintains a reasonable expectation of privacy in information aggregated from the long-term monitoring of his movements without affecting a trespass remains unanswered.[65] In 2013, the Supreme Court hinted that the inquiry into reasonable expectations of privacy does not turn on what "information a hypothetical third person" may learn, but rather what "a person generally expects from third parties."[66]

---

second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[61] *See* Price, *supra* note 55, at 262 n.110 (collecting cases discussing reasonable expectations of privacy as applied to digital technology).

[62] *See* United States v. Knotts, 460 U.S. 276, 285 (1983) (holding no reasonable expectation of privacy when defendant drove on public roads because police officer following defendant would reveal the same information).

[63] *See* Oliver v. United States, 466 U.S. 170, 178–80 (1984) (finding no reasonable expectation in open fields, which are areas beyond the home and its curtilage).

[64] Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area[]' . . . constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

[65] In *Jones*, the majority held that the case was decided on the trespass theory; however, at least five Justices, in scattered concurrences, also stated their displeasure with long-term monitoring. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in part) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

[66] *See* State v. Tate, 849 N.W.2d 798, 806 n.13 (Wis. 2014) ("'[I]ntroducing a trained police dog to explore the area around the home in hopes of discovering incriminating evidence' constitutes a search because it is not part of a 'customary invitation' to attempt entry . . . ." (quoting Florida v. Jardines, 133 S. Ct. 1409, 1416 (2013)).

In this light, the Supreme Court's tracking-technology decisions help guide our understanding of what is reasonable in the CSLI context.[67] The Supreme Court analyzed the reasonableness of tracking-device technology in *United States v. Knotts*, where the government placed a tracking device inside a barrel and tracked it through public roads to a cabin.[68] In analyzing the privacy implications of the use of the tracking device without a warrant, the Court began with the assertion that a person's expectation of privacy must be "justifiable," "reasonable," or "legitimate."[69] The Court found that the government did not violate any reasonable expectation of privacy by monitoring the barrel within an automobile, even remotely, on the public road to the cabin because the police could have obtained the same information by following defendant's vehicle.[70] It is important to note that Knotts did not challenge the fixation of the tracking device to the barrel.[71] Thus, the court did not expound on a trespass theory. This issue arose again in *United States v. Karo*, where the facts resembled those of *Knotts*, except that, in *Karo*, the government continued to track the barrel once it was inside the defendant's home.[72] The Court built a privacy fence at the entrance of one's home:

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, *whether* a

---

[67] *See generally Knotts*, 460 U.S. 276; United States v. Karo, 468 U.S. 705 (1984); *Kyllo*, 533 U.S. 27; *Jones*, 132 S. Ct. 945.

[68] *See Knotts*, 460 U.S. at 277–80.

[69] *Id.* at 280.

[70] *Id.* at 282 ("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.").

[71] *Id.* at 286 (Brennan, J., concurring) ("I think this would have been a much more difficult case if respondent had challenged, not merely certain aspects of the monitoring of the beeper installed in the chloroform container purchased by respondent's compatriot, but also its original installation.").

[72] *See Karo*, 468 U.S. at 716.

> particular article—or a person, for that matter—is in an individual's home at a particular time.[73]

Then, in *Kyllo v. United States*, the Supreme Court emphasized that a person's home is not completely free from remote monitoring.[74] Instead, only information about the intimacies of one's home obtained through the use of technology not in general public use is prohibited.[75] Eleven years later, the Court revisited its tracking-device precedent in *United States v. Jones*.[76] In *Jones*, the government affixed a tracking device to the defendant's vehicle without a warrant and without a valid court order.[77] The government tracked the vehicle remotely for twenty-eight days.[78] The Supreme Court determined that the government trespassed on Jones's property and, thus, held narrowly, leaving undecided whether the long-term monitoring of the location of Jones's vehicle constituted a search.[79] It was the *Jones* decision that reinvigorated the trespass theory of privacy protections.[80]

---

[73] *Id.* (emphasis added).

[74] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[75] *Id.* (holding that government's use of a thermal imaginer revealing intimacies of one's home violated Fourth Amendment because the device was not in general public use).

[76] 132 S. Ct. 945 (2012).

[77] *See id.* at 948.

[78] *Id.*

[79] *Id.* at 954 ("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."); *id.* at 953 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.").

[80] *See* Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 808–10 (2013) [hereinafter *Real-Time and Historic Location Surveillance*] ("[W]e have two conceptions of Fourth Amendment search, both of which were satisfied, but no answer as to what law enforcement must know or do before conducting that search."); *see also* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C.J.L. & TECH. 431, 458 (2013) [hereinafter *After* United States v. Jones] ("*Jones* can be read as a return to the more flexible approach of *Katz*, which is more likely to get the 'right' result in a particular case, even if it also leaves the doctrine a bit nebulous for future cases.").

B. *The Third-Party Doctrine*

The third-party doctrine has a significant impact on a person's reasonable expectation of privacy.[81] Until 1976, the cases discussing the third-party doctrine involved undercover agents and government informants.[82] Then, in *United States v. Miller*, the Court extended the doctrine to business records held by third parties.[83] In *Miller*, a subpoena directed Miller's banking institution to disclose his banking records to the government.[84] The district court held this constituted a seizure and stated that the subpoena compelled the "production of a man's private papers."[85] The Supreme Court affirmed the appellate court's reversal, holding that the documents were not Miller's "private papers" because the banking institution was a party to the documents and thus no trespass occurred.[86] In rejecting any reasonable expectation of privacy in the documents, the Court crafted an *ad hoc* inquiry to determine whether a person holds a reasonable expectation of privacy in documents controlled by third parties: "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[87]

Three years later, the Supreme Court performed this *ad hoc* inquiry in *Smith v. Maryland*, where it relied on *Miller* and determined that the numbers recorded from a pen register installed by a telephone company at the request of law enforcement was not a search

---

[81] For discussions regarding the development of the third-party doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566–71 (2009). *See also* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 7–11 (2014).

[82] *See* On Lee v. United States, 343 U.S. 747, 753 (1952) (holding that no search occurred because the defendant voluntarily communicated plans to the undercover agent); Lopez v. United States, 373 U.S. 427, 440 (1963) (holding that recorded statements made to IRS agent were not unlawfully obtained); Lewis v. United States, 385 U.S. 206, 212 (1966) (holding no Fourth Amendment violation when defendant invited undercover agent into home); *see also* Hoffa v. United States, 385 U.S. 293, 301–03 (1966) (holding no search occurred when defendant revealed incriminating information to another).

[83] United States v. Miller, 425 U.S. 435 (1976).

[84] *Id.* at 438.

[85] *Id.* at 438–39 (citing Boyd v. United States 116 U.S. 616, 622 (1886)).

[86] *Id.* at 440–41.

[87] *Id.* at 442.

under the Fourth Amendment.[88] The Court, relying on *Katz*, determined that a customer has no reasonable expectation of privacy in the phone numbers he dials.[89] The Court essentially based its holding on three key facts: (1) the limited capabilities of pen registers to merely record numbers, (2) public advertising indicating that telephone companies may use pen registers to record the numbers dialed by customers, and (3) the fact that customers voluntarily communicate the numbers dialed to phone companies with these capabilities.[90] Thus, the Court concluded that Smith "voluntarily conveyed" and "exposed" to the phone company the numbers he dialed, which were subsequently recorded by the pen register, thereby removing his reasonable expectation of privacy in that information.[91] Presently, the third-party doctrine eliminates a person's claim to a reasonable expectation of privacy:

> It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . .[92]

C. *Statutes*

The brass-tacks inquiry under the Fourth Amendment is whether a search occurred and, if so, whether the government performed it reasonably.[93] "The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the

---

[88] Smith v. Maryland, 442 U.S. 735, 738 (1979); *Id.* at 745.

[89] *Id.* at 745.

[90] *See id.* at 742.

[91] *Id.* at 744.

[92] United States v. Jacobsen, 466 U.S. 109, 117 (1984) (holding that the Fourth Amendment is not implicated if the Government does not exceed scope of the search performed by a non-government third party).

[93] *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (noting that the "touchstone" of the Fourth Amendment is reasonableness); *see also* United States v. Davis, 785 F.3d 498, 522 (11th Cir. 2015) (en banc) (Jordan, J., concurring)

search and the extent to which the search intrudes upon reasonable privacy expectations.'"[94] In the context of federal statutes, there is a "strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable.'"[95] Thus, it is not surprising that the government has aggressively requested access to CSLI under the guise of statutory permissibility.[96]

1. THE SCA AND HISTORICAL CELL-SITE LOCATION INFORMATION

The statute relied on most often is the Stored Communications Act ("SCA"). The SCA was one of many extension to the Communications Act, which provides basic privacy rights for consumers by requiring all communications carriers "to protect the confidentiality of proprietary information of, and relating to . . . [its] customers . . . ."[97] Originally, Congress passed the Communications Act in response to Justice Taft's decision in *Olmstead v. United States*.[98]

(stating that even if a search occurred, the search was reasonable because of the procedures set forth in 18 U.S.C. § 2703(d) (2012)).

[94] Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015), *quoted in Davis*, 785 F.3d at 522 (Jordan, J., concurring).

[95] United States v. Watson, 423 U.S. 411, 416 (1976), *quoted in Davis*, 785 F.3d at 523 (Jordan, J., concurring); *see also* United States v. Carpenter, No. 14-1572, 2016 WL 1445183, at *7 (6th Cir. Apr. 13, 2016) (noting that "society itself—in the form of its elected representatives in Congress—has already struck a balance" on the reasonableness of privacy expectations in CSLI through 18 U.S.C. § 2703(d)).

[96] Judge Smith conservatively estimated that, in 2006, the "number of electronic surveillance orders issued at the federal level . . . substantially exceed[ed] 10,000." *June 2010 Hearing*, *supra* note 10, at 80 (statement of Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas); *see also Real-Time and Historic Location Surveillance*, *supra* note 80, at 810 ("[L]aw enforcement requested some information from cell phone providers over 1.3 million times in 2011 . . . .").

[97] 47 U.S.C. § 222(a) (1934).

[98] *See* Howard J. Kaplan et al., *The History and Law of Wiretapping*, 3 AMERICANBAR.ORG (Apr. 18–20 2012), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf; *see also* Olmstead v. United States, 277 U.S. 438, 466 (1928) ("[O]ne who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.").

Years later, Congress passed the Wiretap Act.[99] In doing so, Congress placed significant limitations on the circumstances under which a wiretap may be used to obtain information due to a wiretap's ability to record content and non-content information.[100] Applications for "[w]iretaps are often referred to as 'super-warrants' because of the additional requirements beyond probable cause necessary for their issuance."[101] Notably, the Wiretap Act limits the use

---

[99] 18 U.S.C. §§ 2510–2522 (1968).

[100] *See id.* § 2518; *see also* Kaplan et al, *supra* note 98, at 4–5 (discussing that Congress enacted a new wiretap statute after the Supreme Court's decision in *Katz*); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified at 18 U.S.C. §§ 2510–2522) ("In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized . . . .").

[101] *In re* U.S. for and Order, 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010). The requirements for an application for a wiretap are as follows:

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

of a wiretap to a thirty-day period before another request must be made.[102]

Subsequently, Congress enacted the Electronic Communications Privacy Act ("ECPA").[103] While the Wiretap Act covered only "wire" and "oral" communications,[104] the ECPA purportedly regulates all electronic communications.[105] The ECPA introduced provisions regulating the use of pen registers and trap-and-trace devices.[106] Both pen registers and trap-and-trace devices can be authorized by court order if the information sought is "relevant to an ongoing criminal investigation."[107] Like a wiretap, a pen register or trap-and-trace device may only be used for a limited duration before seeking judicial re-approval.[108]

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

18 U.S.C. § 2518(1).

102 *See* 18 U.S.C § 2518(5).

103 *In re* U.S. for Order Directing a Provider of Elec. Commc'n, 534 F. Supp. 2d 585, 593 (W.D. Pa. 2008) (noting that the ECPA was a "major overhaul" of the Wiretap Act of 1968), *vacated*, 620 F.3d 304 (3d Cir. 2010).

104 *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified at 18 U.S.C. §§ 2510–2522).

105 *See Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22*, JUSTICE INFO. SHARING, U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUDICIAL ASSISTANCE (July 30, 2013), https://it.ojp.gov/default.aspx?area=privacy&page=1285 ("The ECPA, as amended, protects wire, oral, and electronic communications . . . .").

106 *See* 18 U.S.C. §§ 3121–3127; *see also id.* § 3127(3) (defining "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"); *id.* § 3127(4) (defining "trap and trace device" as a "device or process which captures the incoming electronic or other impulses which identify the originating number").

107 *See id.* § 3123(a)(1).

108 *See id.* § 3123(c). The ECPA was amended further by the Communications Assistance for Law Enforcement Act ("CALEA") to prevent the disclosure of a subscriber's location information when the use of a pen register or trap-and-trace

Shortly after, Congress passed the SCA to regulate the disclosure of electronic information stored by third parties.[109] These provisions, however, are not clear.[110] For example, the SCA has multiple provisions allowing for the disclosure of the same stored communications. Under subsection (c)(1)(A), the SCA allows disclosure of communication information upon the issuance of a warrant based on probable cause.[111] However, subsection (c)(1)(B) refers the reader to subsection (d) of the same provision, which states that a court "shall issue" an order directing a cell-service provider to disclose electronic communications only if the government "offers 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."[112] The standard of proof of subsection (c)(1)(A), probable cause, and that of subsection (c)(1)(B), relevance to an ongoing criminal investigation, are clearly different. Thus, the government can obtain the same type of stored electronic information with a showing of probable

---

device is authorized. *See* 47 U.S.C. § 1002(a)(2) (stating that information obtained using a pen register or trap-and-trace device "shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)").

[109] *See* 18 U.S.C. §§ 2701–2712.

[110] *Compare id.* § 2703(c) ("Records concerning electronic communication service or remote computing service – (1) A governmental entity 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 (not including the contents of the communications) only when the government entity – (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; (B) obtains a court order for such disclosure under subsection (d) of this section; or (C) has the consent of the subscriber or consumer to such disclosure . . . ."), *with id.* § 2703(d) ("Requirements for Court Order – A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and 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.").

[111] *Id.* § 2703(c)(1)(A).

[112] *Id.* § 2703(d).

cause or a lesser showing of specific and articulable facts.[113] Why would law enforcement ever seek to satisfy the probable cause standard under subsection (c)(1)(A) if it can obtain the same stored communications under a relevance standard of subsection (c)(1)(B)?[114]

This language has unsurprisingly led to confusion.[115] Some courts hold that the SCA expressly regulates the disclosure of CSLI to the government.[116] These courts reason that the SCA regulates the access of "stored" communications, and section (c) states that the government may "require" a service provider to disclose a customer's records or "other information pertaining to a subscriber . . . ."[117] Thus, the government considers CSLI to be "other information," and the SCA merely requires the government to meet

---

[113] *See In re* U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 287 (4th Cir. 2013) (stating that the standard under § 2703(d) is "essentially a reasonable suspicion standard"); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013) ("The 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant.").

[114] For a discussion of the different standards, see 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, 151–57 (2012). *See also* Freiwald, *supra* note 11, at 697 ("The D order standard, then, permits much broader inquiries into a much wider range of targets.").

[115] *In Re* U.S. for Order Directing a Prov. of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010) ("[W]e are stymied by the failure of Congress to make its intention clear.").

[116] *See In re* U.S. for Historical Cell Site Data, 724 F.3d at 615 ("[A]s long as the Government meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order."); *see also In re* U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (holding that HCSLI "clearly satisfies" the requirements under § 2703(c) and, thus, an order was appropriate); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 147 (E.D.N.Y. 2013) (holding no reasonable expectation of privacy in cellphone location); United States v. Madison, No. 11-60285, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) (Rosenbaum, J.) (holding Fourth Amendment was not implicated under third-party doctrine); *In re* U.S. for an Order Authorizing Use of a Pen Register, 2009 WL 159187, at *3 (S.D.N.Y. Jan. 13, 2009) (finding that a "cell phone falls squarely within the statutory definition of the term 'tracking device'").

[117] 18 U.S.C. § 2703(c).

the criteria set forth in § 2703(d).[118] To satisfy § 2703(d) a court must decide whether the holder of the record is a "provider" of electronic communications, whether CSLI is a stored "record," and whether CSLI is content or non-content information.[119]

As I did with the technology behind CSLI, threshold questions of the definitions used by the SCA and how CSLI fits those definitions must be addressed. For starters, the SCA encompasses all records concerning electronic communication services.[120] It defines "electronic communication services" as including "wire or electronic communications."[121] A "wire communication" is defined as "any aural transfer" made through the use of the wires.[122] An "aural transfer" is a communication that contains the "human voice."[123] An "electronic communication" is "any transfer" of data transmitted by "wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ."[124] The definition of "electronic communication" also explicitly excludes any "communication" from a "tracking device (as defined in section 3117 of this title) . . . ."[125] Comparatively, there is no exclusion for tracking-device communications under the definition of wire communications. The complicating element of CSLI is that it can be created from both wire and electronic communications. For example, when a call is made or received, the communication falls under a wire communication because it involves the human voice. But, a text

---

[118] *See In re* U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d at 79–80.

[119] *Id.* The content-versus-non-content debate regarding CSLI was articulated in the En Banc Amicus Curiae Brief of the National Association of Criminal Defense Lawyers in Support of Appellant Quartavious Davis at 20, United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015) (No. 12-12928). *See also* Freiwald, *supra* note 11, at 740–43 (explaining that *Smith* did not create a rule allowing non-content disclosure).

[120] *See* 18 U.S.C. § 2703(c).

[121] 18 U.S.C. § 2510(14).

[122] *See id.* § 2510(1) (defining "wire communication" as "any aural transfer made in whole or in part through the use of . . . wire, cable, or other like connection").

[123] *See id.* § 2510(18).

[124] *Id.* § 2510(12).

[125] *Compare id.* § 2510(1) (no exclusion of tracking devices), *with id.* § 2510(12) (noting that electronic communication excludes "any communication from a tracking device (as defined in section 3117 of this title)").

message or other non-aural communications falls under the definition of electronic communication. Thus, if a cellphone is characterized as a tracking device, then the SCA cannot be a vehicle for obtaining records of CSLI created from the electronic communications; however, the SCA can be used to obtain the records for CSLI from wire communications. At this point, the discussion of the definitions is merely to illustrate the potential complications with applying the SCA to CSLI.

2. THE HYBRID THEORY AND PROSPECTIVE CELL-SITE LOCATION INFORMATION

In addition to requesting from service providers the location information they store, the government also requests that location information of a target cellphone be disclosed at some time in the future. This type of tracking information is termed Prospective Cell-Site Location Information ("PCSLI"). To obtain this information, the government combines statutes to facilitate the search.[126] This "Hybrid Theory" has had limited success in the courts.[127]

The Hybrid Theory combines provisions of the Communications Assistance for Law Enforcement Act ("CALEA"), the pen-register statute, and the SCA.[128] Under this theory, the government argues that the pen-register statute—18 U.S.C. § 3127(3)—authorizes it to record "signaling information" from a user's phone, including CSLI.[129] Unfortunately for the government, the CALEA prohibits the disclosure of call-identifying information that "may disclose the

---

[126] *See* United States v. Espudo, 954 F. Supp. 2d 1029, 1034 (S.D. Cal. 2013) (describing PCSLI as "the acquisition of data for a period of time *going forward from* the date of the order" (emphasis in original)).

[127] *See id.* at 1035 (stating "the majority of federal courts examining . . . [PCSLI] mandate that the government make a showing of probable cause"); *see also In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 n.6 (3d Cir. 2010) (collecting cases discussing hybrid theory).

[128] *See In re* U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 205 (E.D.N.Y. 2008) (discussing the statutes selected and utilized by the government to argue that PCSLI is constitutional); *see also In re* App. for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 747 (S.D. Tex. 2005).

[129] *See In re U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F. Supp. 2d at 205.

physical location of the subscriber" when a pen register or trap-and-trace device is used.[130] By itself, this limitation prevents the disclosure of a user's location information or, in the case of a cellphone, CSLI. To get around this limitation, the government relies on provisions from the SCA to allow service providers to disclose CSLI as "other information" when the standards previously discussed are met.[131] The government merely argues that PCSLI is a type of "other information" and relies on the SCA. Other courts, however, recognize that the SCA cannot apply to PCSLI.[132] These courts reason that because CSLI "permits the tracking of the movement of a person or object," it turns the phone into a tracking device, which requires a warrant.[133] Further, with a tracking device, a judge must

---

[130] 47 U.S.C. § 1002(a).

[131] *See* 18 U.S.C. § 2703(d).

[132] *See id.* § 3117; *see also In re* Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 900 (S.D. Tex. 2014) (holding that SCA is not a vehicle for obtaining prospective CSLI); *In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 (3d Cir. 2010) (holding that CSLI is not a tracking device because CSLI is a wire communication and, thus, not an electronic communication under which tracking devices are excluded). During the legislative hearings, one party commented that the definition of "tracking device" is broad enough that it could be "read as including . . . cellular equipment." *Electronic Communications Privacy Act, Hearing Before the H. Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the H. Comm. on the Judiciary*, 99th Cong. 99 (1985) (statement of John Stanton, Chairman Telocator Network of America), https://www.justice.gov/sites/default/files/jmd/legacy/2014/04/29/-hear-50-1985.pdf.

[133] *See In re* Order Authorizing Prospective and Continuous Release of Cell Site Location, 31 F. Supp. 3d 889, 896 (S.D. Tex. 2014); *In re U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 310; *see also In re* U.S. for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *6, *7 (S.D.N.Y. Jan. 13, 2009) (unpublished); *In re* U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005); United States v. White II, 62 F. Supp. 3d 614, 624–26 (E.D. Mich. 2014) (Nov. 24, 2014) (holding that a cellphone becomes a tracking device when request is filed and need for "installation" becomes superfluous when records are requested). *But see* United States v. Booker, 2013 WL 2903562, at *1, *10 (N.D. Ga. June 13, 2013) ("The general nature of the location information sought by the government here—merely the cell towers and sectors used during each call—does not bring it into the realm of Fourth Amendment

limit the monitoring to forty-five days.[134] Yet, there is no temporal limitation within the SCA. Thus, it seems illogical for Congress to enact strict regulations for location information from a physically applied tracking device, but have no similar regulation when that same information is obtained by merely requesting it from a third party. If the SCA allows the disclosure of CSLI, then the SCA has superseded the Wiretap Act.

However, if we go back to the definitional status of CSLI, it may be too broad to consider all cellphone communications to be "tracking device" communications.[135] As discussed previously, a literal reading of the SCA and its definitions means that a cellphone *is not* a tracking device when a "wire communication" is involved, but it *is* a tracking device when an "electronic communication" is involved.[136] Importantly, deciphering which CSLI data point is the result of an electronic communication versus a wire communication occurs only after the information has been disclosed by the third party. Thus, there is no way to know which information is protected until after the information is disclosed to the government, unless the service provider is required to pre-screen information.

With technological improvements and the "world's most effective tracking device"[137] within five feet of a person at any given time,[138] it is unlikely that the government will seek to physically affix a tracking device when the same—if not better—location infor-

---

protection."); *In re* Smartphone Geo. Data App., 977 F. Supp. 2d 129, 149–50 (E.D.N.Y. 2013) (holding that a cellphone does not meet the definition of "tracking device" under 18 U.S.C. § 3117).

134 *See* FED. R. CRIM. P. 41(e)(2)(C).

135 *See In re* U.S. for Order PCSLI on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 460 n.55 (S.D.N.Y. 2006) (noting that "if a cell phone is a tracking device by virtue of the fact that it provides cell site information, then *all* information provided by a cell phone to a cell phone service provider . . . fall[s] outside of the scope of 'electronic communication'").

136 *Compare* 18 U.S.C § 2510(1), *with id.* § 2510(12).

137 *See White II*, 62 F. Supp. 3d at 625 (quoting JULIA ANGWIN, DRAGNET NATION 141 (2014)); *see also* United States v. Jones, 123 S. Ct. 945, 963 (2012) (Alito, J., concurring).

138 *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("[N]early three-quarters of smart phone users report being within five feet of their phones most of the time . . . .").

mation is available under the lesser burden of "specific and articulable facts."[139] If the statutes apply, then CSLI, which is arguably more invasive than information gathered using traditional tracking devices, is authorized (1) on a lesser showing than probable cause, (2) for an undetermined amount of time, and (3) without any provisions requiring judicial renewal.[140]

III. REASONABLE EXPECTATIONS OF PRIVACY IN CSLI

A. *Privacy Expectations and CSLI*

Having reviewed the technology behind CSLI and the statutory regimes, an analysis of the privacy expectations in CSLI can now occur. To have a reasonable expectation of privacy, (1) a person must subjectively believe that his activity or information is private, and (2) society must recognize that belief as "legitimate," "justifiable," or "reasonable."[141] Despite scholars arguing that judges have historically been bad predictors of what society expects as reasonable,[142] many arguments for and against a reasonable expectation of privacy in CSLI have been proffered. Specifically, the Third, Fourth, Fifth, Sixth, and Eleventh Circuits have addressed this issue and have failed to reach a consensus.[143] Likewise, state supreme

---

[139] 18 U.S.C. § 2703(d); *see also 2014 Wiretap Report: Intercept Applications Down Slightly* (July 1, 2015), http://www.uscourts.gov/news/2015/07/01/2014-wiretap-report-intercept-applications-down-slightly (finding wiretap applications decreased by 1% from 2013 to 2014).

[140] *Compare* 18 U.S.C. § 2703, *with* FED. R. CRIM. P. 41(e)(2)(C).

[141] *See* United States v. Knotts, 460 U.S. 276, 280 (1983).

[142] *See* Price, *supra* note 55, at 263 ("Empirical studies have also demonstrated that the Supreme Court is at best unreliable when it comes to determining the actual privacy expectations of the average person.").

[143] *See In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 (3d Cir. 2010); United States v. Graham 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75; *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that HCSLI is covered under the plain text of the SCA); United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015) (en banc); United States v. Carpenter, No. 14-1572, 2016 WL 1445183, at *7 (6th Cir. Apr. 13, 2016).

courts that have addressed the issue fail to agree on the rationale as to why a reasonable expectation of privacy in CSLI exists.[144]

The trouble, of course, is in determining exactly what privacy expectation exists in CSLI and whether the third-party doctrine vitiates that expectation. Courts performing the *Katz* test disagree on whether society is willing to recognize a justifiable privacy interest in CSLI.[145] Specifically, the Eleventh Circuit relied on the Fifth Circuit's decision in *In re United States for Historical Cell Site Data* to determine that there is no reasonable expectation of privacy in CSLI.[146] The Fifth Circuit claimed that all cellphone users understand that a "cell phone must send a signal to a nearby tower" to make or receive a call.[147] The Eleventh Circuit concurred, reasoning that "users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage."[148]

Courts holding to the contrary reason that the fact that a user knows his cellphone communicates with cell sites "does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes."[149] As the Florida Supreme

---

[144] *See* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014); *see also* State v. Earls, 70 A.3d 630 (N.J. 2013); State v. Tate, 849 N.W.2d 798, 813 (Wis. 2014) (avoiding reasonable expectation of privacy inquiry because judge's order supported issuance on probable cause standard).

[145] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *Compare Davis*, 785 F.3d at 511–13 (holding no reasonable expectation of privacy in CSLI), United States v. Madison, No. 11-60285, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012), United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (finding no reasonable expectation of privacy in data voluntarily conveyed by phone), *and In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (same), *with Graham*, 796 F.3d at 344 (holding reasonable expectation of privacy exists in CSLI), Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (same), *and In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010).

[146] *See* 724 F.3d at 613–14 (finding no reasonable expectations of privacy in CSLI).

[147] *In re U.S. for Historical Cell Site Data*, 724 F.3d at 613 (holding no reasonable expectation of privacy in HCSLI because information is business record of service provider).

[148] *Davis*, 785 F.3d at 511.

[149] *Tracey*, 152 So. 3d at 522.

Court put it, "Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion . . . places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace."[150] Furthering the argument that a cellphone is a necessity, users have begun to disconnect landlines in favor of their cellphones,[151] and research suggests society has an expectation of privacy in their location information.[152]

Evidencing this point are statements by Supreme Court Justices, holdings of state supreme courts, and legislation passed by some states. In 2010, the Supreme Court stated that the pervasiveness of cellphone use "might strengthen the case for an expectation of privacy."[153] In fact, ninety percent of U.S. households use wireless cell service.[154] Further, in *Riley v. California*, the Supreme Court expressed concern over the privacy infringements that HCSLI can impose: "Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements

---

[150] *Id.* at 523; *see* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

[151] From 2003 to 2013, families with only wireless phone service increased from less than 5% to almost 40%. *See* Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, July–December 2013*, NAT'L HEALTH INTERVIEW SURVEY EARLY RELEASE PROGRAM (July 2014), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201407.pdf.

[152] *See* Lauren E. Babst, Note, *No More Shortcuts: Protect Cell Site Location Data with a Warrant Requirement*, 21 MICH. TELECOMM. & TECH. L. REV. 363, 378–79 (2015) (collecting PEW research studies suggesting the amount of privacy society expects in location information and cellphone use); *see also Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 11, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/pi_2014-11-12_privacy-perceptions_03/ (last visited Feb. 10, 2015) (suggesting fifty percent of adults surveyed believed the details of their physical location over time were very sensitive information); *Davis*, 785 F.3d at 538 (Martin, J., dissenting) ("82% of adults 'feel as though the details of their physical location gathered over a period of time' is 'very sensitive . . . .'").

[153] City of Ontario v. Quon, 560 U.S. 746, 760 (2010).

[154] *Wireless Quick Facts*, *supra* note 38.

down to the minute, not only around town but also within a particular building."[155]

Although the Supreme Court has yet to express an opinion on CSLI, the state supreme courts of Massachusetts, Florida, and New Jersey have held that law enforcement's warrantless request for CSLI violated their respective state constitutions.[156] In 2014 alone, nine states passed legislation requiring probable cause before the government can obtain CSLI.[157] As of October 2015, a total of eighteen states require probable cause, rather than a relevance standard, before obtaining CSLI.[158]

Some courts consider whether the contracts between users and cellphone companies waive an expectation of privacy in CSLI.[159] Some opine that even if users did read the privacy policies, those policies may not explain the information turned over to the government.[160] Courts have also held that obtaining CSLI is unconstitutional because the Fourth Amendment protects privacy in the home.

---

[155] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (holding search incident to arrest forbade officers from searching contents of cellphone without a warrant).

[156] *See* Commonwealth v. Augustine, 4 N.E.3d 846, 868 (Mass. 2014); *see also* State v. Earls, 70 A.3d 630, 644 (N.J. 2013); Tracey v. State, 152 So. 3d 504 (Fla. 2014).

[157] Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU (last updated Jun. 30, 2014), https://www.aclu.org/blog/technology-and-liberty-national-security/status-location-privacy-legislation-states (Virginia, Utah, Montana, Minnesota, Massachusetts, Maryland, Maine, Iowa, Indiana, Illinois, and Colorado).

[158] Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, ACLU (last updated Oct. 13, 2015), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015.

[159] United States v. Graham 796 F.3d 332, 345 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 ("There is no evidence that Appellants here read or understood the Sprint/Nextel policy."); *see also* Jon Leibowitz, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf; Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A., (Oct. 20 2010, 12:17 PM) http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.

[160] The language found in the cell-service provider's privacy policies is general in nature. *See Verizon Full Privacy Policy*, (last visited Jan. 17, 2015) (stating Verizon collects and uses Cell-Site Location Information), http://www.verizon.com/about/privacy/policy/#infoadv; *AT&T Privacy Policy*, (last visited Jan.

Because CSLI is collected and then the location is ascertained by a human only after its disclosure, the argument goes that learning whether someone is in their home through CSLI at a particular time is an unreasonable search.[161] The Eleventh Circuit disagreed, finding that no violation occurs when a person is located in his home. It relied on *Smith* to reason that Smith's location was obtained by the fixing of a pen register and Smith was in his home.[162] Thus, at least *Smith* does not support this proposition. But, as one scholar notes, the *Smith* decision seems at odds with cellphone technology: "[A]s more people do have an expectation of privacy in information they've turned over to third parties, it's the *Smith* decision, and not the expectation of privacy, that becomes unreasonable."[163] Supporting this counterargument is the fact that the *Smith* decision did not focus on the location of a person in its analysis.

Also, a landline phone number is strictly tied to a location—a home or business. A cellphone, on the other hand, can be anywhere with a viable signal. Thus, the privacy implications of CSLI should be analyzed in accord with the tracking device used in *Knotts* or *Karo* because, like that tracking device, the cellphone is not intimately associated with the home directly but can find its way there. "Indiscriminate 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."[164]

17, 2015) (stating AT&T collects and uses Cell-Site Location Information), http://www.att.com/Common/about_us/privacy_policy/print_policy.html#location. The Metro PCS privacy policy is devoid of any language explaining that CSLI will be turned over under the SCA. *See* https://www.metropcs.com/content/metro/en/mobile/metro/termsconditions/termsconditionsdetails.privacy.html (last visited Feb. 10, 2015).

[161] *See* Tracey v. State, 152 So. 3d 504, 518 (2014) (illustrating that cases allowing CSLI to be freely obtained would require analysis of data and suppression of data where user located in home under the Supreme Court's rationale in *Karo*).

[162] *See* United States v. Davis, 785 F.3d 498, 511–12 (11th Cir. 2015) (en banc).

[163] Hanni Fakhoury, Smith v. Maryland *Turns 35, But Its Health Is Declining*, ELEC. FRONTIER FOUND. (Jun. 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining.

[164] United States v. Karo, 468 U.S. 705, 716 (1984).

B. *The Third-Party Doctrine and CSLI*

The applicability of the third-party doctrine to CSLI significantly affects a person's reasonable expectation of privacy. Whether a reasonable expectations of privacy exists in CSLI involves the applicability of the third-party doctrine. At least with respect to jurisdictions covering Florida, the courts are split as to its applicability.[165] While the Florida Supreme Court read the third-party doctrine narrowly in *Tracey v. State*,[166] the Eleventh Circuit, in *Davis*, held that the third-party doctrine precludes a reasonable expectation of privacy in information conveyed to service providers.[167] In cases involving CSLI, there appears to be a disparity in interpretation over the term "voluntarily conveyed."[168] Like the Florida Supreme Court, other courts have read *Miller* and *Smith* narrowly, warning that a broad reading of "voluntary communications" fails to adequately consider privacy expectations in the digital age.[169] These courts find support in dicta provided by many Supreme Court Justices, which repeatedly indicate displeasure with the third-party doctrine and its

---

[165] *Compare* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (holding that a reasonable expectation of privacy exists in PCSLI), *with In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2014) ("[A]s long as the Government meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order."). *See also In re* U.S. for Orders Pursuant to Title 18, U.S.C. Section 2703(d) 509 F. Supp. 2d 76, 80 (D. Mass. Sept. 17, 2007) ("Because historical cell site information clearly satisfies" the requirements under section 2703(c), an order is appropriate.); *In re* Smartphone Geolocation Data App., 977 F. Supp. 2d 129, 145 (E.D.N.Y. 2013) (holding no reasonable expectation of privacy in cellphone location); United States v. Madison, No. 11-60285, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) (Rosenbaum, J.).

[166] *Tracey*, 152 So. 3d at 526.

[167] *Davis*, 785 F.3d at 511 ("[L]ike the bank customer in *Miller* and the phone customer in *Smith*, Davis has no subjective or objective reasonable expectation of privacy in [the service provider's] business records . . . .").

[168] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

[169] *See Tracey*, 152 So. 3d at 525; *see also* United States v. Powell, 943 F. Supp. 2d 759, 770 (E.D. Mich. 2013); *In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010).

deficiencies when applied in the modern era.[170] Recently, in his concurrence in *Riley*, Justice Alito called for a "new balancing of law enforcement and privacy interests," stating that "we should not mechanically apply the rules used in the predigital era to the search of a cell phone."[171]

Because the third-party doctrine emphasizes the voluntary communication of actions or words to third parties, the technology behind CSLI is brought to the forefront of the debate. This is why it was crucial to painstakingly detail CSLI technology in Part I. Put simply, those advocating for the inapplicability of the third-party doctrine argue that cellphone users do not voluntarily convey CSLI.[172] Despite the fact that companies collect and utilize CSLI to improve the services provided, CSLI is different than the bank records in *Miller* and the phone numbers in *Smith*. Distinguishing *Miller*, Susan Freiwald argues, "Cell phone users, however, do not voluntarily convey location data to providers, or tell their providers to record it. Quite unlike bank statements, which are designed for customer review, customers can hardly know what location data their providers store . . . ."[173]

Consider the following: unlike the active process of entering a phone number, which was at issue in *Smith*, a user does not enter his

---

[170] *See* U.S. Dept. of Justice v. Reporters Comm. For Freedom of Press, 489 U.S. 749, 763 n.14 (1989) ("Almost every such fact, however personal or sensitive, is known to someone else. Meaningful discussion of privacy, therefore, requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure." (quoting another source)); *see also* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine "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."); Riley v. California, 134 S. Ct. 2473, 2496–97 (2014) (Alito, J., concurring).

[171] 134 S. Ct. at 2496–97 (Alito J., concurring) (holding that search incident arrest doctrine did not allow for the search of files stored on cellphone).

[172] *Tracey*, 152 So. 3d at 522 (noting that CSLI is not voluntarily conveyed to the company in "any meaningful way" (quoting *In re U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317)); *see* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era,* PEW RESEARCH CTR. (Nov. 11, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ ("91% of adults in the survey 'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies.").

[173] Freiwald, *supra* note 11, at 737.

location or the location of the target recipient's phone when placing a call with a cellphone. The number itself is not tied to any location. Because CSLI is a by-product of the user making the call, it is a passive process that the phone does automatically. Without looking at the records, it would be impossible for a user to know what cell tower his phone was registering with at a particular time. Therefore, it is improbable that the user could communicate his precise location and cell site, even if the user wanted to.

Moreover, the *Smith* decision involved only the numbers he dialed out and whether he had a privacy interest in the phone numbers that he chose to call from his home phone.[174] If the *Smith* decision is said to control CSLI, then it should only extend to CSLI created by the user of the phone and not information received by the phone without the user's actions. CSLI created when a call is received is not "voluntarily conveyed" as interpreted by *Smith*. The only way the *Smith* decision can apply to all CSLI is if it can be said that a person has no reasonable expectation of privacy in his location by virtue of having a cellphone on his person.

Another writer distinguishes CSLI from the voluntary conveyances in *Miller* and *Smith* by arguing that CSLI is an "automated electronic intermediary."[175] Under this theory, service providers are merely a conduit used to facilitate communications between parties who are the originator and target of the communication. Whereas the pen registers at issue in *Smith* replaced human operators, cellphone service is completely automated. Even if it can be said that cellphone transmissions were once subject to human operators, it is nearly impossible to imagine the number of human operators it would take to transmit texts, weather updates, e-mails, calls, and internet connections.[176] There is no human that is involved in the process of CSLI until that information is requested by the government.

---

[174] *See* Smith v. Maryland, 442 U.S. 735, 738 (1979) (discussing the installation and use of a pen register, which records only the numbers dialed from a user's phone).

[175] John P. Collins, Note, *Third Party Doctrine in a Digital Age*, at 8, http://www.nyls.edu/documents/justice-action-center/student_capstone_journal/cap12collins.pdf.

[176] *International Smartphone Mobility Report – Jan. '15*, INFORMATE MOBILE INTELLIGENCE (Mar. 25, 2015), http://informatemi.com/blog/?p=133 (finding that the average smartphone user in the United States "makes or answers 6 phone calls

Essentially, under this theory, the third-party doctrine should be applicable only if there is a person that the information conveyed to. Simply being able to ascertain the records of a completely autonomous process should be insufficient to satisfy the third-party doctrine.

An interesting twist in the analysis of the third-party doctrine is that the government requires service providers to track the location of cellphones for emergency-response purposes. Service providers store CSLI not only for their own use, but also because it is mandated by statute.[177] The rules promulgated by the Federal Communications Commission ("FCC") mandating minimum accuracy requirements of CSLI affect the debate.[178] In 2011, the FCC found that seventy percent of 911 calls were placed from cellphones.[179] In response, the FCC promulgated rules to increase the accuracy of location information when a cellphone user places a call to 911.[180] Phase One of the FCC rules requires service providers to provide emergency personnel with the phone number and the cell site that transmitted the call.[181] Phase Two requires service providers to provide the latitude and longitude of the phone, which must be accurate to within 50 to 300 meters.[182]

By requiring third-party service providers to create location services for the government, the government has essentially turned all participating service providers into government agents.[183] It seems disingenuous for the government to require a third party to monitor the location of cellphones and then to use the third-party doctrine to

---

per day, sends and receives 32 texts and spend 14 mins. On Chat/VOIP apps per day").

[177] *See* 47 C.F.R. § 20.18.

[178] *See id.*

[179] *911 Wireless Services*, F.C.C., https://www.fcc.gov/consumers/guides/-911-wireless-services (last visited Mar. 22, 2016) [hereinafter FCC].

[180] BEDELL, WIRELESS, *supra* note 11, at 386.

[181] *See* BEDELL, CELLULAR NETWORKS, *supra* note 9, at 306.

[182] *Id.*; *see also* 47 C.F.R. § 20.18(h); FCC, *supra* note 179.

[183] United States v. Feffer, 831 F.2d 734, 737 (7th Cir. 1987) ("The government may not do, through a private individual, that which it is otherwise forbidden to do. Accordingly, if in light of all the circumstances a private party conducting a serach must be regarded as an instrument or agent of the government, the fourth amendment appies to that party's actions.") (citing Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)); *see also* United States v. Malbrough, 922 F.2d 458, 461–62 (8th Cir. 1990).

request the records that the government compels the third party to create in the first place.

IV. SOLVING CSLI: MOSAICS, TRACKING DEVICES, AND A NEW INTERPRETATION OF THE THIRD-PARTY DOCTRINE

The above discussion clearly raises more questions than it answers, and it is understandably confusing. Some of the nation's highest courts cannot pin down the arguments for and against the disclosure of CSLI without a warrant. Many courts and scholars advocate for clarity from the legislature,[184] merely asking for clearly worded statutes or protection from CSLI disclosure without a warrant.

Some courts find guidance in the "Mosaic Theory."[185] The "Mosaic Theory" encompasses the view that, by sifting through the entirety of a person's HCSLI, the government is able to create an intimate depiction of the person's life.[186] It is as though the government can press rewind and watch a person's movements without forming a suspicion of criminal activity until months or years after the data points were created.[187] In rejecting privacy expectations in CSLI,

---

[184] *See* Pell & Soghoian, *supra* note 114, at 163–70; United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015) (en banc) ("Davis and *amici* advance thoughtful arguments for changing the underlying and prevailing law; but these proposals should be directed to Congress and the state legislatures rather than to the federal courts."); Freiwald, *supra* note 11, at 686–87 ("[P]rivacy-invading practices will continue until either the courts step up or Congress steps in to revise the ECPA.").

[185] United States v. Graham 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75. For a thorough critique of the Mosaic Theory, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (concluding that the Mosaic Theory should be rejected by the courts).

[186] The Mosaic Theory had its beginnings in *United States v. Kirschenblatt*, where then-judge Learned Hand identified the difference between specific and broad information collection: it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for every which may incriminate him . . . ." *See* 16 F.2d 202, 203 (2d Cir. 1926). Subsequently, it was defined in *C.I.A. v. Sims* as "'[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information its the proper context.'" 471 U.S. 159, 178 (1985) (quoting Halkin v. Helms, 598 F.2d 1, 9 (D.C. Cir. 1978)).

[187] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will

Third Circuit did not reject the premise that CSLI can "be used to approximate the past location of a person."[188] CSLI is quite precise, and its precision is increasing in modern society. Even the Florida Supreme Court, which found a reasonable expectation of privacy in CSLI, rejected the Mosaic Theory as "not a workable analysis."[189] Yet, a panel of the Fourth Circuit adopted this approach in *United States v. Graham*:[190]

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[191]

Still, others find light in the tracking-device statutes alluded to above.[192] And some scholars find the third-party doctrine serves a substitutive role in modern crimes, is relatively easy to apply, and provides necessary clarity for law enforcement.[193]

However, that the Supreme Court should interpret HCSLI and PCSLI collectively and alter the *Katz* inquiry to include the third-party doctrine as one factor in the reasonable-expectation-of-privacy

---

be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

[188] *In re* U.S. for Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312 (3d Cir. 2010).

[189] However, in making this determination, the Florida Supreme Court relied on the lower court's analysis of the Mosaic Theory in *Graham v. United States*, which was overturned and is now being reheard en banc. *See* Tracey v. State, 152 So. 3d 504, 520 (Fla. 2014); United States v. Graham 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75; *see also* Kerr, *supra* note 185, at 346 (finding the Mosaic theory to be "very difficult to administer").

[190] *See Graham*, 796 F.3d at 360. *But see* United States v. Davis, 785 F.3d 498, 515 (11th Cir. 2015) (en banc) ("Historical cell site location data does not paint the 'intimate portrait of personal, social, religious, medical, and other activities and interactions' that Davis claims.").

[191] United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2015), *quoted in Graham*, 796 F.3d at 348.

[192] *See supra* note 132 (collecting cases discussing CSLI and the tracking device theory).

[193] *See* Kerr, *supra* note 185, at 566–71.

test, rather than treating it as an exception.[194] Here's how it can be done: First, the distinction between HCSLI and PCSLI must be eliminated. Drawing this distinction creates a logically untenable dissimilarity because cellphone technology does not distinguish between the two. The technology behind CSLI transmission does not support the distinction. Maintaining the distinction between HCSLI and PCSLI also poses analytical difficulties. Obtaining HCSLI under the SCA requires that the HCSLI be a record of "other information." If so, at first blush it seems rather straight-forward to apply the SCA. What is confusing is the skepticism that courts express when PCSLI is requested. As mentioned above, courts appear quick to find that the request for PCSLI is a request for tracking device information. Why is it any different with HCSLI? Is a cellphone any less of a tracking device merely because the information has already been recorded? It must also be stressed that, presumably, the SCA operates under the auspice that the third party is voluntarily recording CSLI. However, as mentioned above, the government requires service providers to maintain cell sites, which can accurately locate a cellphone.

Further, drawing a distinction between HCSLI and PCSLI lures courts into the difficult task of determining where PCSLI ends and where HCSLI begins. United States Magistrate Judge Stephen William Smith articulated this conundrum: "How is 'historical' to be defined—one second after transmission? One hour? One day? One month?"[195] Is the defining point the date of the request for information? Is it the date that the order is issued? Also illustrative of the false dichotomy is that a request for PCSLI is necessarily a request for HCSLI from the third party. Logically, even when PCSLI is sought, the CSLI is transmitted to the service provider nanoseconds before it is conveyed to the government. Thus, at the time of conveyance, it is HCSLI.[196] The fact that the data simply was not stored

---

[194] *See* Freiwald, *supra* note 11, at 689 ("[I]f the courts take too long to address new technology, they create the risk not only that the technology they do address will be obsolete but also 'that the Fourth Amendment will never really catch up.'").

[195] *June 2010 Hearing*, *supra* note 10, at 86.

[196] For a more probing analysis of the "instantaneous storage theory," see *In re* Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 892–96 (S.D. Tex. 2014).

at the time of the request should be irrelevant to categorization.[197] The character or nature of the data does not change; it remains CSLI. Regardless of whether the data is stored at the time of the request, the specificity of a person's location information does not change. "The SCA makes no distinction between historical and prospective"[198] CSLI, and there is nothing less private about CSLI that *has already been* stored by a service provider than CSLI that *will be* stored by the service provider.

By removing the HCSLI/PCSLI distinction, courts can wrestle with the more pressing issue of whether a reasonable expectation of privacy exists in CSLI in toto.[199] The doctrines from the pre-digital age fail to adequately address CSLI. Technology is constantly in a positive feedback system: new technology is released, it becomes incorporated into society, then it happens again and again. "[I]f a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate that technology, the effect will be that the Fourth Amendment matters less and less over time."[200]

---

[197] *See Real-Time and Historic Location Surveillance*, *supra* note 80, at 831 ("Whether police receive my location information as I 'create' it or a week later, assuming the same level of detail for both, the information—and therefore the benefit to law enforcement and the privacy implications—are identical.").

[198] United States v. Booker, No. 1:11-CR-255-1, 2013 WL 2903562, at *6 (N.D. Ga. June 13, 2013).

[199] Some courts currently recognize that HCSLI and PCSLI should be treated similarly. *See* United States v. White II, 62 F. Supp. 3d 614, 619 (E.D. Mich. 2014); *Booker*, No. 1:11-CR-255-1, 2013 WL 2903562, at *7 (N.D. Ga. June 13, 2013) ("While this [CSLI] is 'prospective' in the sense that the records had not yet been created at the time the Order was authorized, it is no different in substance from the historical cell site location information . . . ."); Commonwealth v. Augustine, 4 N.E.3d 846, 854 n.9 (Mass. 2014) (analyzing HCSLI without distinguishing PCSLI); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (upholding reasonable expectation in the location of a person's cell phone on state constitutional grounds); *In Re* U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008) (noting PCSLI becomes HCSLI as soon as it is recorded).

[200] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 125 HARV. L. REV. 476, 527 (2011).

As the doctrine exists now, voluntary conveyance to a third party makes any expectation of privacy unreasonable in the conveyed information.[201] This interpretation of Supreme Court precedent forces courts into the minefield that has become the aforementioned jurisprudence of CSLI. The third-party doctrine should be analyzed as one factor in the reasonable-expectation-of-privacy inquiry rather than as an exception to the inquiry's application. The digital age has changed the definition of "voluntary conveyance" such that treating "secrecy as a perquisite for privacy" is no longer tenable.[202] The Supreme Court cases that apply the third-party doctrine to business records discuss the voluntary conveyance of information to a third party—a person. As described above, the extension of the third-party doctrine to business records evolved out of cases where the defendant made affirmative statements to another person.[203] It is easy to conceptualize voluntary conveyance in this manner. A tells B incriminating statements, trusting that B will not repeat them. But, there is nothing preventing B from repeating A's statement except B's will. When the third-party communication involves incidental information, voluntary conveyance becomes more difficult to define. CSLI is the perfect example. Certainly, location information is conveyed to the service provider when a call is placed or received, but is it really a voluntary conveyance as it has been articulated in third-party doctrine jurisprudence?

Perhaps it can be quite easy. CSLI can be compared to the address and return address on envelopes sent through the mail. The Supreme Court held years ago that there is no privacy in that information.[204] But, again, this seems to be more of a voluntary act sim-

---

[201] *See After* United States v. Jones, *supra* note 80, at 434–42 (discussing the third-party doctrine cases and the implications of *United States v. Jones*).

[202] United States v. Jones, 132 U.S. 945, 957 (2012) (Sotomayor, J., concurring); *see also* RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006) ("Informational privacy does not mean refusing to share information with everyone.").

[203] *See supra* Part III.

[204] *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("letters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

ilar to *Smith* than the passive communication of CSLI from a cellphone. It seems that the incidental communications accompanying technological interactions make the third-party doctrine so difficult to apply.

Rather than treating the third-party doctrine as an exception to a user's reasonable expectation of privacy, courts should utilize it as one factor in determining whether a search has occurred. The *A.B.A. Standards for Criminal Justice: Law Enforcement Access to Third Party Records* ("LEATPR") is a similar proposal.[205] Stephen Henderson applied these standards to CSLI.[206] Under the LEATPR standards, "law enforcement would need a warrant to access over twenty-four hours of location information, could access a lesser period of location information using a lesser court order, and could access a record indicating location at a single point in time for any legitimate law enforcement purpose."[207] These standards consider the area of privacy expectations that the third-party doctrine currently overlooks.

The LEATPR brings to the forefront that there exists degrees of privacy in information. Specifically, the LEATPR is organized around four factors: (1) the purpose of the initial transfer of the electronic information to a third party and the societal interest served by its disclosure, (2) the extent to which the information is personal and whether it is disclosed to third parties other than for the purpose of facilitating electronic transactions, (3) the accessibility of that information by other parties, and (4) the state of the existing law.[208] Based on these factors, the amount of privacy a person expects in a particular document or electronic information can be determined. The approach taken by the LEATPR is "mildly mosaic," as Stephen Henderson put it, because the LEATPR evaluates the electronic in-

---

[205] *See* A.B.A. STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013) [hereinafter LEATPR].

[206] *See also Real-Time and Historic Location Surveillance*, *supra* note 80, at 810. For a discussion on the commentary to the LEATPR, see Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875 (2014) [hereinafter Freiwald, *Light in the Darkness*].

[207] *See Real-Time and Historic Location Surveillance*, *supra* note 80, at 810.

[208] *See* LEATPR, *supra* note 205, at 12.

formation being obtained by looking to the circumstances surrounding the data.[209] For example, when determining the initial level of privacy expectations a point of electronic data should be afforded, the standards ask several questions like "why is this information in the hands of the third party?" and "is the transfer of this information to the third party something to be wary of chilling?"[210]

To me, the LEATPR standards read as thoughtfully prepared guidelines, but the practical application of these standards is a concern. If read as an insightful inquiry into the concerns surrounding the disclosure of digital communications, then these guidelines provide a fertile resource. As Susan Freiwald posits, "The LEATPR Standards provide a framework for members of Congress interested in drafting an entirely new law or amending the SCA to address law enforcement's compelled disclosure of location records . . . ."[211] Informing the legislature of concerns is a world apart from asking courts to implement these guidelines into workable analytical rules. Further, a significant problem with the guidelines is that, if implemented, they would not apply to the "acquisition of information contemporaneous with its generation or transmission . . . ."[212] In other words, the guidelines would maintain the distinction between HCSLI and PCSLI.

Despite the LEATPR having been published in 2012, federal courts of appeals and state supreme courts continue to struggle to apply reasonable expectations of privacy and the third-party doctrine to technology. This suggests that these guidelines are not a practical implementation. Perhaps, sometimes less is more. In the case of voluntary communications to third parties, changing the *Katz* inquiry to add a third prong creates an applicable analytical structure. Therefore, the modified *Katz* inquiry would be performed as follows:

---

209 *See Real-Time and Historic Location Surveillance*, *supra* note 80, at 823–24.

210 *Id.* at 813.

211 Freiwald, *Light in the Darkness*, *supra* note 206, at 908.

212 LEATPR, *supra* note 205, at § 25-2.1(e). Stephen Henderson argues that the default protections of the LEATPR should apply to prospective location information because the privacy intrusion and the interests of law enforcement are the same as that of historic location records. *See Real-Time and Historic Location Surveillance*, *supra* note 80, at 831.

> (1) Is there a subjective expectation of privacy in the information?
>
> (2) Was the information voluntarily conveyed to a third party, and to what degree of voluntariness if at all?
>
> (3) Notwithstanding that conveyance, is society prepared to accept that expectation as reasonable?

The addition of the voluntariness prong incorporates the third-party doctrine into the reasonable-expectation-of-privacy inquiry without unmooring it from prior applications. Consider *Miller* under the new inquiry. Asking the degree of voluntariness Miller had in communicating his account information to the bank reveals that Miller affirmatively and actively conveyed this information to use the services of the bank.[213] There was an intention by Miller to convey his bank records to the bank employee. Regardless of whether he intended that information to be kept within the bank, his act of conveyance was voluntary. Likewise, in *Smith*, Smith's conveyance of phone numbers to the telephone company was affirmative and voluntary.[214] He intended to convey the phone numbers he dialed to the company so that his call could be properly directed to the intended recipient. The analysis of these voluntary acts informs the third prong of the analysis: whether society is prepared to accept that expectation as reasonable.

Consider obtaining CSLI—either HCSLI or PCSLI—under the new reasonable-expectations-of-privacy analysis. Assuming a subjective expectation of privacy exists, the next inquiry is to what degree is CSLI voluntarily conveyed to the third party? The language of "to what degree" allows courts to consider the nature and means that the information is communicated to a third party. In this way, courts will be better able to adequately address the conveyance of incidental electronic communications. CSLI falls squarely within this type of electronic communication. Thus, at least for CSLI communicated by a cellphone to a service provider, the new inquiry properly addresses the technology behind its use.

---

213 *See* United States v. Miller, 425 U.S. 435, 438–39 (1976).

214 *See* Smith v. Maryland, 442 U.S. 735, 738, 745 (1979).

V. SILENCE, STINGRAYS, AND CSLI

A. *The Silent Use of Independent Cell Site Simulators*

In addition to obtaining CSLI from third-party service providers, the government also uses cell-site simulators. When media coverage of the government's use of cell-site simulators boomed a few years ago, scholarship emerged discussing the secrecy surrounding cell-site simulators.[215] In fact, despite the claimed prevalent use of cell-site simulators, there are few reported cases.[216] The controversy surrounding the use of cell-site simulators escalated when it became known that "prosecutors throw cases out rather than have the use of cell-site simulators revealed in court."[217]

Stingray systems function similarly to cell sites, which were discussed in Part II. In fact, Stingrays mimic cell sites. Over the past few years, the media have outed the government's use of cell-site simulators.[218] According to the Department of Justice, law enforcement agencies use Stingrays either (1) "to help locate cellular devices whose unique identifiers are already known to law enforcement," or (2) "to determine the unique identifiers of an unknown device . . . ."[219] As discussed above, a cellphone communicates its location to a cell tower by registering with it.[220] A cell-site simulator

---

[215] *See also* Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134 (2013).

[216] *See generally* United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012); *In re* U.S. for an Order Auth. the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *In re* U.S. for an Order Relating to Telephones Used by Suppressed, No. 15-M-0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015).

[217] Nicky Woolf, *Lawmakers demand details on federal use of Stingray phone surveillance*, THE GUARDIAN (Nov. 9, 2015), http://www.theguardian.com/us-news/2015/nov/09/congress-stingray-surveillance-jason-chaffetz-elijah-cummings.

[218] *See* Heath, *supra* note 8; Erin Kelly, *Federal agents will no longer use 'Stingray' cellphone trackers without warrants*, USA TODAY (Oct. 21, 2015), http://www.usatoday.com/story/news/2015/10/21/federal-agents-no-longer-use-stingray-cellphone-trackers-without-warrants/74337250/.

[219] U.S. DEP'T OF JUSTICE, *supra* note 33, at 1.

[220] *See* U.S. DEP'T OF JUSTICE, ELEC. SURVEILLANCE UNIT, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW 40–41 (rev. 2005),

works by superseding the signal emitted from a service provider's cell site within an area, causing all mobile devices to register with it instead of the cell site.[221] Stingrays essentially trick a cellphone into thinking the Stingray is the closest cell site, and the cellphone then transmits its location information to the Stingray instead of the service provider's cell site. Typically, cell-site simulators canvas only a small area, and thus, law enforcement attach them to aircraft and vehicles to increase the coverage area and facilitate the location of a targeted device.[222]

A cell-site simulator enables its operator to locate a device, intercept calls and text messages, and send fake calls or texts to the target device to trigger the cellphone to transmit its location.[223] Practically speaking, the difference between CSLI obtained through a cell site owned by a third party and CSLI obtained via a cell-site simulator used by the government is merely the presence or absence of the third party service provider.

B. *Is CSLI Obtained By Stingrays A Search?*

Unlike CSLI obtained from a service provider, there is no record to obtain from a third party when a cell-site simulator is used. Thus, the statutory provisions of the SCA can be relied upon.[224] However, there exist regulations promulgated by some of the agencies that use

---

http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf [hereinafter ELECTRONIC SURVEILLANCE MANUAL]; *see also June 2010 Hearing*, *supra* note 10, at 14 (testimony of Matt Blaze, Associate Professor, University of Pennsylvania) (stating that, without registration data, the cell-service provider "won't know how to get calls to you").

[221] *See In re* U.S. for an Order Relating to Telephones Used by Suppressed, No. 15-M-0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015).

[222] *See FBI operating fleet of surveillance aircraft flying over US cities*, THE GUARDIAN (June 2, 2015), http://www.theguardian.com/us-news/2015/jun/02/fbi-surveillance-government-planes-cities.

[223] *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 11 (2014) [hereinafter *Your Secret StingRay's No Secret Anymore*].

[224] *See In re* Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 678 (S.D. Tex. 2015) ("[E]ven though the StingRay and the tower dump may both ultimately yield the same information—the number or identifier of the cell phone used by a criminal suspect—the manner of acquiring that information is very different, and entails a very different legal analysis.").

cell-site simulators. In 1997, the Department of Justice required prosecutors to obtain an order under the pen-register statute before using cell-site simulators.[225] In 2005, the Department of Justice stated that "a pen register/trap and trace order *must* be obtained by the government before it can use" a cell-site simulator.[226] Recently, in September 2015, the Department of Justice changed its policy to require a warrant before a cell-site simulator is used.[227] The Department of Homeland Security followed suit.[228] This policy change, however, is not without its critics.[229]

At least for now, law enforcement's use of cell-site simulators is self-policing. Lawmakers introduced a bill dubbed the "Cell-Site Simulator Privacy Act of 2015," which would require all law enforcement agencies to obtain a warrant before using a cell-site simulator, regardless of the policy decisions of individual agencies.[230] Until this occurs, there may be Fourth Amendment implications regarding the use of CSLI obtained via a cell-site simulator.

Comparing CSLI obtained from a third-party service provider to CSLI obtained from a cell-site simulator used by government reveals one prominent distinction. In the former, the third party is performing the data collection. In the latter, the government is directly performing the locating. On its surface, it seems to be a more compelling argument to say that the use of cell-site simulators is a

---

[225] *See Your Secret StingRay's No Secret Anymore*, *supra* note 223, at 23–26 (citing ELECTRONIC SURVEILLANCE MANUAL, *supra* note 220, at 40–41).

[226] *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 220, at 41 (emphasis added).

[227] *See Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators: Increase Privacy Protections and Higher Legal Standards to Be Required*, U.S. DEP'T OF JUSTICE (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators; *see also* USE OF CELL-SITE SIMULATOR TECHNOLOGY, *supra* note 33, at 1–7 (2015).

[228] U.S. DEP'T OF HOMELAND SEC., DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY, POLICY DIRECTIVE 047-02 (Oct. 19, 2015), https://www.dhs.gov/sites/default/files/publications/Department%-20Policy%20Regarding%20the%20Use%20of%-20Cell-Site%20Simulator%-20Technology.pdf.

[229] Neema Singh Guliani, *The Four Biggest Problems with DHS's New Stingray Policy*, ACLU (Oct. 22, 2015), https://www.aclu.org/blog/free-future/four-biggest-problems-dhss-new-stingray-policy.

[230] *See* H.R. 3871, 114th Cong. (1st Sess. 2015).

greater violation of the Fourth Amendment than the former. Specifically, the signal from the cellphone transmitting directly to a cell-site simulator is eerily similar to a tracking device, which many courts have supported in PCSLI cases.[231] An argument also exists that the use of a cell-site simulator allows for the type of long-term, non-invasive tracking that the concurring justices in *Jones* opined about. Either way, there is no third-party for the government to rely on for the disclosure of the records. There is simply no third-party intermediary. Thus, the core principal of the third-party doctrine—the presence of a third party—is absent. Accordingly, it seems that the unmitigated use of cell-site simulators would be an unreasonable search under the Fourth Amendment.[232]

The use of a cell-site simulator is a tracking device. The only difference is that there no physical installation occurring. It is true that the Court in *Jones* held that a Fourth Amendment violation occurred because law enforcement agents committed trespass when they affixed a tracking device to a vehicle without a valid warrant.[233] However, putting aside the potential Fourth Amendment implications that accompany physical trespass of affixing a tracking device, not requiring a warrant to obtain CSLI makes the tracking-device statute virtually useless. If the government can obtain the same, if not more accurate, location information from a cellphone by using a cell-site simulator, then what is the point of the tracking-device statute and its protections? It becomes the legal equivalent of a vestigial organ.

---

[231] *See In re* U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device, 2009 WL 159187, at *3 (S.D.N.Y. Jan. 13, 2009) (finding that a "cell phone falls squarely within the statutory definition of the term 'tracking device'").

[232] *See* Boyd v. United States, 116 U.S. 616, 635 (1886) ("It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.").

[233] *See* United States v. Jones, 132 S. Ct. 945, 948 (2012).

If CSLI can be obtained via a cell-site simulator without a warrant, then the circumstances in which the government would actually install a tracking device is limited to situations where the government is concerned with tracking the location of a particular item—a car or contraband—rather than the location of a person. Tracking a particular item is significantly less invasive than tracking a person surreptitiously through his passively created CSLI. Yet, a warrant would still be required to affix a tracking device to an object.[234] On the other hand, CSLI would be obtainable without one simply because no physical installation occurs. It is for that reason, that the concurring justices in *Jones* and the courts in CSLI cases are rightfully concerned, and some have relied upon the Mosaic Theory in finding a Fourth Amendment violation.[235]

Like CSLI obtained from third-party service providers, cell-site simulators should be analyzed under the modified *Katz* test. Despite the fact that there is no service provider to act as an intermediary, the privacy expectations still depend on CSLI, not on who is receiving the data. Although no third party is used when the government uses a cell-site simulator, a person's reasonable expectation of privacy is affected in the same manner. This is a function of CSLI. The cellphone emits CSLI, and it does so indiscriminately. It can be argued that if a person knows his cellphone uses CSLI to function, then he can be said to be voluntarily communicating it to anyone who may "want[] to look . . . ."[236] It wouldn't matter if the government or a service provider is collecting that information.[237]

The reverse can also be argued. CSLI can be considered an entirely passive process insofar as the user does not voluntarily convey his location in any meaningful way simply by having a cellphone on his person. In either case, it becomes apparent that the central focus is the CSLI and its communicative process—not the recipient. Thus, it is the incidental communication of CSLI that should control this

---

234 *See* 18 U.S.C § 3117(a).

235 *See Jones*, 132 S. Ct. at 957 (Alito, J., concurring); *id.* at 954 (Sotomayor, J., concurring); United States v. Graham 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75.

236 United States v. Knotts, 460 U.S. 276, 281 (1983).

237 Not analyzed further in this note is how the Supreme Court's holding in *Kyllo* would affect the inquiry depending on whether cell-site simulators are in public use or not. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

debate. The modified *Katz* test introduced above applies to cell-site simulators because the reasonable expectation of privacy depends on the privacy a person has in CSLI. This, in turn, stems from an analysis of whether CSLI is voluntarily communicated to third-party service providers. If courts address these issues with an understanding of the technology, then the result should be the same under either technology.

CONCLUSION

Courts must stop waiting for the technological dust to settle, so to speak, before addressing the issues that accompany it; technology will never stop changing. Many courts have attempted to apply existing precedent to new technology. As this discussion of CSLI illustrates, the doctrines used are ill-applied. The third-party doctrine addresses scenarios where information is affirmatively communicated from one person to another, and whether there is any reasonable expectation that the person told will not communicate that information to law enforcement. Quite simply, the CSLI debate illustrates that it does not adequately address passive electronic communications.

As a review of the technology illustrates, whether the government obtains information from a third-party service provider or from using a cell-site simulator, courts need to eliminate the fictional HCSLI–PCSLI dichotomy. The technology behind cellphone communications makes clear that there is no technological difference between HCSLI and PCSLI. Further, modifying the *Katz* test to incorporate the third-party doctrine would lead to uniformity among the courts—at least in the analytical framework applied to CSLI cases. Doing so integrates an inquiry similar to that of the LEATPR guidelines without the impracticality of a verbose, multi-factor test. Finally, there should be no difference in expectations of privacy between the use of a third-party service provider and cell-site simulator. Courts need to focus the inquiry on CSLI and not the technology using the CSLI. Society and its expectations of privacy are ever-changing. Whether privacy is reasonably expected in CSLI or not,[238]

---

[238] *See Jones*, 132 S. Ct. at 962 (Alito, J., concurring) ("[E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

there must be some uniformity among the courts so that society has guidance. The modified *Katz* inquiry proposed here within provides such analytical uniformity.