2017

When That Hotline Bling: The Tracking Device in Your Pocket

Charles A. Shadle

When That Hotline Bling:

The Tracking Device in Your Pocket

Part I. Introduction

Thirty years ago the United States Supreme Court dismissed the notion that law enforcement could conduct continuous surveillance on individuals without a warrant. Justice Rehnquist stated that if "twenty-four hour surveillance of any citizen of this country" became a possibility, "there will be time enough . . . to determine whether different constitutional principles may be applicable."[1] Today, the government now has the capability of conducting such around-the-clock surveillance on unwitting individuals without obtaining a warrant to do so. This technology is called cell-site location information (CSLI) and cell phone users generate it without their knowledge.[2] It is time for the Supreme Court to recognize the reasonable expectation of privacy in this information and protect cell phone users across the United States.

Most people are aware that their cell phone has to connect to a cell tower in order for a call to be made; cell-site location information is the information that is retained by the service provider that identifies which tower connected the last call.[3] Using this information, law enforcement is able to plot a route that the individual has taken over a period of time.[4] While this technology might not be able to precisely track a user's movements in a sparsely covered area

[1] United States v. Knotts, 460 U.S. 276, 283 (1983) (internal citations omitted).
[2] *See* Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ ("In its most recent annual report, AT&T said it received 64,703 requests for CSLI in 2014. And just in the first six months of this year, Verizon says it received more than 21,000 requests. That is, in 2015, a single carrier received more than 100 requests daily…").
[3] *See* United States v. Graham, 2015 U.S. App. LEXIS 13653, at *15-16 (4th Cir. 2015).
[4] *See Id.* at *16-17.

due to the distance between cell towers, in urban areas the cell sites "tend to have smaller radii of operability" allowing them to more accurately place an individual.[5] Service providers today are competing to provide an increasing coverage quality, leading to the placement of towers that cover areas as small as 40 feet resulting in increased precision at these sites.[6]

The Stored Communications Act, passed by Congress in 1986, has given law enforcement the capability to obtain electronic information generated by users of various technologies.[7] Law enforcement must "offer[] specific and articulable facts" to receive a court order compelling the disclosure of the CSLI by the service provider.[8] The Senate has described this standard as "higher than a subpoena, but not a probable-cause warrant."[9] In order to obtain CSLI, law enforcement must make a request upon a magistrate judge who has the ability to deny the request if the standard is not met.[10] Unfortunately though, law enforcement has been able to meet this standard typically with ease allowing them to access this sensitive information.

Law enforcement officials have made so many requests of AT&T, the service provider has been forced to establish a separate department solely tasked with responding to orders to compel disclosure of CSLI.[11] The periods that they seek to obtain CSLI for are not confined to a small window in time; rather, the government has obtained cell-site location information for periods of as long as 221 days without a warrant obtained by a showing of probable cause.[12] If the government obtained this quantity of location information about you, what might it uncover?

---

[5] *Id.* at *17.
[6] *See Id.* at *36.
[7] Stored Communications Act, 18 USCS § 2701.
[8] 18 USCS § 2703(d).
[9] *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010).
[10] *See Id.* at 306.
[11] *See* Lauren E. Babst, Note, *No More Shortcuts: Protect Cell Site Location Information With a Warrant Requirement*, 21 MICH. TELECOMM. TECH. L. REV. 363, 375 (2015).
[12] *See* United States v. Graham, 2015 U.S. App. LEXIS 13653, at *10 (4th Cir. 2015).

Do people "reasonably expect that their movements will 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."[13] CSLI has the ability to track your movements to and from a place of worship, medical appointments, and other sensitive location information that the public would not to expect the government to obtain without a warrant. The unfortunate reality is that the government is obtaining this information nearly every day without a warrant.

Before discussing the case law surrounding the privacy rights implicated in CSLI, it is important to note the prevalence of cell phone use in modern American society. As of January 2014, 99% of American adults own a cell phone and as of October 2014, 64% of American adults own a smart phone.[14] Cell phones are no longer considered a luxury either; 84% of people making less than $30,000 a year own a cell phone and 90% of people making between $30,000 and $49,999 own a cell phone.[15] Furthermore, one in five cell phone owners has turned off the location feature on their cell phone.[16] Yet turning off the location feature does not prevent CSLI from being generated.

Some courts and commentators suggest that by using a cell phone, society has voluntarily given up whatever constitutional right to privacy that may have existed through cell-site location information.[17] It is time for the Supreme Court to weigh in on this pressing issue affecting the privacy interests of all cell phone users in the United States and recognize a reasonable

---

[13] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[14] *Mobile Technology Fact Sheet*, PewInternet.org, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited October 3, 2015).
[15] *Id.*
[16] *Id.*
[17] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); Scott A. Fraser, Comment, *Making Sense of New Technologies and Old Law: A New Proposal for Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571 (2012); Christopher Fox, Comment, *Checking In: Historical Cell Site Location Information and the Stored Communications Act*, 42 SETON HALL L. REV. 769 (2012); Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701 (2012).

expectation of privacy in CSLI. This paper will survey the applicable Supreme Court precedent in part II, the Circuit Courts that currently do not recognize a reasonable expectation of privacy in CSLI in part III, and the Circuit Court that does recognize a reasonable expectation of privacy in CSLI in part IV. In part V, this paper will argue that the third party doctrine is not applicable to the records stored by cell phone service providers, cell phone users have a subjective expectation of privacy in their cell-site location information, and that expectation is a reasonable one in society's eyes. This paper will also make the argument that CSLI is precise enough to implicate concerns expressed in the Supreme Court's most recent case law on the subject.

Part II. Fourth Amendment Constitutional Background

A. Foundation

The Fourth Amendment protects against unreasonable searches and seizures of persons, houses, papers, and effects.[18] Before the government is allowed to perform a search of these things they must obtain a warrant by a showing of probable cause.[19] The United States Supreme Court in *Katz v. United States* laid down the test for when a warrant is required before a search can be conducted. Katz was convicted of transferring wagering information via telephone in violation of a federal statute.[20] The government obtained incriminating evidence by placing a recording device outside of the telephone booth at which Katz was making his phone calls.[21] The government argued that this method was not a search within the meaning of the Fourth Amendment because a telephone booth was not a constitutionally protected area. The Supreme

[18] U.S. CONST. amend. IV.
[19] *Id.*
[20] *See* Katz v. United States, 389 U.S. 347, 348 (1967).
[21] *See Id.*

Court disagreed stating "the Fourth Amendment protects people, not places."[22] Thus, it was a search for which a warrant was required because the government "violated the privacy upon which [Katz] justifiably relied . . ."[23] *Katz* has been transformed into a two prong test as to whether a warrant is required: first, whether there is a subjective expectation of privacy and second, whether that expectation is objectively reasonable.[24]

B. Third Party Doctrine

While *Katz* established the test for determining whether a warrant is required, the Court has also acknowledged that what a person exposes to the public does not receive Fourth Amendment protection.[25] *United States v. Miller* helped develop a doctrine known as the third party doctrine, which governs this exception to the protections of the Fourth Amendment. Miller was convicted of making alcohol and distributing it illegally.[26] At trial, the government introduced evidence of checks that Miller had deposited at a bank, but the Court of Appeals ruled that Miller had a Fourth Amendment protection in his bank records if obtained by an illegal subpoena.[27] When the question reached the Supreme Court it reasoned that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . ."[28] The Court noted that the information had been "voluntarily conveyed" in the "ordinary course of business," and as such Fourth Amendment protection was not warranted.[29]

[22] *Id.* at 351.
[23] *Id.* at 353.
[24] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).
[25] *See* Katz v. United States, 389 U.S. 347, 351 (1967).
[26] *See* United States v. Miller, 425 U.S. 435, 436 (1976).
[27] *See Id.* at 436-37.
[28] *Id*. at 443.
[29] *Id*. at 442.

This doctrine was subsequently applied to telephone records in *Smith v. Maryland*. A robbery victim was receiving menacing calls from someone claiming to be the robber.[30] In response, law enforcement installed a pen register at the telephone company which recorded the numbers dialed from a suspect's home.[31] The defendant was convicted in part because of the evidence obtained through this method of investigation.[32] The Court, using the language of the third party doctrine, explained that the defendant had no reasonable expectation of privacy when he dialed the telephone numbers.[33] The Court took into consideration telephone users' knowledge of how telephones worked in determining that there was no reasonable expectation of privacy.[34]

C. Modern Applications

Katz has remained the test that is applied to different surveillance technologies as the government has become more creative with their investigative techniques. In *United States v. Knotts*, law enforcement placed a beeper inside a chloroform container that was then used to track the transportation of the chloroform to defendant's residence.[35] While the defendant argued that this constituted a search under the Fourth Amendment, the Court rejected the argument stating "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[36] In other words, drivers

[30] *See* Smith v. Md., 442 U.S. 735, 737 (1979).
[31] *See Id.*
[32] *See Id.*
[33] *See Id.* at 744.
[34] *See Id.* at 742 ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance…calls on their monthly bills.").
[35] *See* United States v. Knotts, 460 U.S. 276, 278 (1983).
[36] *Id.* at 281.

"voluntarily convey[] to anyone who want[] to look the fact that [they are] traveling over particular roads in a particular direction."[37] The Court then further reasoned that the information in this case could have been obtained by the police through mere visual surveillance, and as such the use of a beeper did not constitute a Fourth Amendment search.[38]

In a case with a similar fact pattern to *Knotts*, in *United States v. Karo*, law enforcement obtained a court order to install a beeper in a shipment of ether to defendant.[39] Law enforcement then tracked the shipment over the course of several days as it changed locations multiple times, and using this information they obtained a warrant to search the final resting place of the shipment.[40] In *Karo*, the Court examined the surveillance of a private residence using the beeper, which was distinguishable from the monitoring of the shipment on public roads in *Knotts*.[41] The Court differentiated the cases by noting that the surveillance in this case was able to "reveal a critical fact about the interior" of the home that could not have been determined unless they had obtained a warrant.[42] Law enforcement, therefore, had violated a reasonable expectation of privacy.[43]

The Supreme Court in *Kyllo v. United States* examined *Katz*'s application to thermal imaging devices. Law enforcement aimed the device at defendant's home under the suspicion that he was growing marijuana, which requires high levels of heat to cultivate.[44] The Court held that such surveillance constituted a search under the Fourth Amendment.[45] The Court focused on the fact that the technology had the capability to see into the home, potentially exposing sensitive

[37] *Id*.
[38] *See Id.* at 282.
[39] *See* United States v, Karo, 468 U.S. 705, 708 (1984).
[40] *See Id*. at 708-09.
[41] *See Id.* at 714.
[42] *Id*. at 715.
[43] *See Id.* at 714-715.
[44] *See* Kyllo v. United States, 533 U.S. 27, 29-30 (2001).
[45] *See Id.* at 40.

information.[46] The Court has also long acknowledged there is a "minimal expectation of privacy that exists, and that is acknowledged to be reasonable" inside of the home.[47] The Court also emphasized the fact that the technology utilized by law enforcement was "not in general public use."[48]

In the most recent case, *United States v. Jones*, decided in 2012, the Supreme Court analyzed a new form of technology under a different theory than the *Katz* framework. In this case, law enforcement suspected the defendant of trafficking drugs and applied for a warrant to attach a GPS device to his car.[49] While his car was parked in a parking lot, law enforcement attached this device, which tracked his movements over a period of 28 days.[50] The majority opinion, written by Justice Scalia, bases the conclusion that a Fourth Amendment search occurred not on the *Katz* test but upon a theory of trespass.[51] Under this theory, due to the fact that the government made a physical invasion onto defendant's property, a search had occurred.[52] Justice Scalia, while relying on a theory of trespass under these circumstances, would still apply the *Katz* framework in "[s]ituations involving merely the transmission of electronic signals without [a physical] trespass . . . ."[53]

The concurring opinions by Justices Sotomayor and Alito in *Jones*, however, base their reasoning on the traditional *Katz* framework. When determining whether a reasonable expectation of privacy exists, Justice Sotomayor takes into consideration the attributes of GPS

[46] *See Id.* at 38 (Stating that the technology could reveal "at what hour each night the lady of the house takes her daily sauna and bath.")
[47] *Id.* at 34.
[48] *See Id.*
[49] *See* United States v. Jones, 132 S. Ct. 945, 948 (2012) (At the time law enforcement placed the device on the car the warrant had expired and the car was not in the jurisdiction in which the warrant had been issued).
[50] *See Id.*
[51] *See Id.* at 951.
[52] *See Id.*
[53] *Id.* at 953.

technology that allow the development of a "precise, comprehensive record of a person's movements."[54] She further suggests that the court should reexamine the validity of the third party doctrine, which she describes as "ill suited to the digital age, in which people reveal a great deal of information to third parties in the course of carrying out mundane tasks."[55]

Justice Alito in his concurrence states that prior to technological advancements, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[56] In order for law enforcement officers in the past to obtain information similar to that obtained using a GPS device, they would have to expend large number of resources – both in terms of financial and personnel resources – whose expenditure was not necessary with the advent of GPS technology.[57] Justice Alito concludes his analysis by reasoning that "society's expectation has been that law enforcement agents and others would not--and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period."[58]

Part III. Circuits That Do Not Recognize a Reasonable Expectation of Privacy in CSLI

While the Supreme Court has not yet weighed in on the lingering question of whether CSLI is entitled to the protections of the Fourth Amendment, the Circuit Courts have begun lining up on either side of the question. The Fifth and Eleventh Circuits have determined that law enforcement does not need to obtain a warrant before compelling disclosure of CSLI.[59] While the Third Circuit also addressed the question of whether a warrant is required, the appeal was from a

[54] United States v. Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring).
[55] *Id.* at 957.
[56] United States v. Jones, 132 S. Ct. at 963 (Alito, J., concurring).
[57] *See Id.* at 963-64.
[58] *Id.* at 964.
[59] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

magistrate judge's denial of an application and thus the warrant requirement was analyzed under an abuse of discretion standard. Therefore, the Third Circuit has seemingly left open the question of the Stored Communication Act's constitutionality as applied to CSLI.[60] While the Sixth Circuit does not analyze an application by the government under the Stored Communications Act, they do analyze whether *Katz* is implicated in law enforcement's tracking of an individual through their cell phone (using a different type of CSLI) and determine that there was no reasonable expectation of privacy.[61]

A. The Fifth Circuit

In *In re United States Application for Historical Cell Site Data*, decided in 2012, the government filed three applications for compelled disclosure of CSLI for three different investigations, each for a period of sixty days.[62] The Court determined that it is required to grant the order under the Stored Communications Act if the Government wishes "(1) to require a provider of electronic communication service or remote computing service (2) to disclose a [non-content] record or other information pertaining to a subscriber to or customer of such service when the Government (3) meets the specific and articulable facts standard."[63] Under the Fifth Circuit's reading, if the government satisfies these requirements, the magistrate judge has no discretion to refuse to grant the order.[64]

Before analyzing CSLI under the *Katz* framework, the Court notes that while the content of communications sent by a third party are protected, the information "which the business needs

[60] *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).
[61] *See* United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).
[62] *See* In re Application of the United States, 724 F.3d at 602.
[63] *Id.* at 607.
[64] *See Id.*

to route those communications appropriately and efficiently," is not.[65] Utilizing this standard, it reasons that CSLI is a business record.[66] The Court focuses on the facts that the service provider is collecting and storing this information for its own purposes and that such information is necessary in order to connect calls.[67]

The Court also rejects the contention that the information was not voluntarily conveyed to the service providers. It notes that contained in the users' agreements with the service providers is a clause that informed the consumer that this information was being retained and stored by the provider. Another clause warns consumers of the possibility that the government may require the service providers to disclose that information.[68] The Fifth Circuit also posits that even if users were not aware of these clauses, their use of a cell phone was voluntary. The government neither requires individuals to use cell phones nor do they require individuals to obtain cell phone coverage from a provider that stores CSLI.[69]

Finally, the Court rejects the contention that society's reasonable expectations of privacy have changed with regards to information conveyed to third parties.[70] Rather, the Court states that the legislature is the proper place to effectuate society's changing expectations.[71] Finishing its analysis, the Court concludes that it "understand[s] that cell phone users may reasonably want their location information to remain private . . . but the recourse for these desires is in the market or the political process."[72]

---

[65] *Id.* at 611.
[66] *See Id.* at 612.
[67] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).
[68] *See Id.* at 613.
[69] *See Id.*
[70] *Id.* at 614.
[71] *See Id.* 614-15.
[72] *Id.* In re Application of the United States, 724 F.3d at 615.

B. Eleventh Circuit

In *United States v. Davis*, which was issued on May 5, 2015, the defendant was indicted for committing seven robberies in a two-month period.[73] Before trial, the government was able to obtain a court order to compel the disclosure of defendant's CSLI under the SCA, which helped show the defendant's movements over that period of time, leading to his conviction.[74] On appeal, the Eleventh Circuit was asked whether CSLI requires Fourth Amendment protection. Like the Fifth Circuit, the Eleventh Circuit begins its analysis by looking at CSLI in the framework of a business record. They state that the defendant cannot claim ownership of the information since it is "lawfully created by a third-party . . . for legitimate business purposes."[75]

In examining the reasonable expectations of cell phone users, the Eleventh Circuit agrees with the Fifth Circuit's reasoning that cell phone users understand how cell phone technology works, and therefore, they can claim no subjective expectation of privacy in the information that allows their calls to be made.[76] Even if a user can claim such a subjective expectation of privacy, the Court finds that, when that expectation is "viewed objectively, [it] is not justifiable or reasonable."[77] Agreeing with the Fifth Circuit, the Court notes that if cell phone users wish to prevent the government from obtaining such information, the proper forum is the legislature and not the judiciary.[78]

While the Eleventh Circuit concludes that CSLI does not receive Fourth Amendment protection, it goes further to examine Justice Alito's concurrence in *Jones*. The Court rejects the argument that Fourth Amendment protection was required under Justice Alito's concurrence,

[73] *See* Davis, United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015).
[74] *See Id.* at 501.
[75] *Id.* at 511.
[76] *See Id.*
[77] *Id.*
[78] *See* Davis, 785 F.3d at 512.

because, unlike GPS, CSLI is not precise enough to give rise to the concerns cited in *Jones*.[79] CSLI merely identifies the particular cell tower from which the call was connected and its use is limited by the strength and density of cell towers that vary depending on service providers.[80] The Court views this technology as far different from the precision and constant flow of information that GPS technologies provide.[81]

Assuming *arguendo* that there was a subjective expectation of privacy, the Court finally examines whether an unreasonable search occurred. The Court relies on the facts that no conversations were heard or recorded, there was no real-time tracking of defendant, and that the SCA contains privacy protections in its provisions in determining that the search was a reasonable one.[82] The Court places additional emphasis on the fact that such records serve a compelling governmental interest in facilitating the apprehension and conviction of criminals in reaching this determination.[83]

C. Third Circuit

Like the Fifth Circuit, the Third Circuit was faced with a situation in which a magistrate judge had denied an application for CSLI under the SCA.[84] In *In re United States Order Directing Provider of Electronic Communication Service to Disclose Records to the Government*, which was decided in 2010, the Court begins its analysis by reviewing the controlling Supreme Court precedent and noting that the holdings in *Knotts* and *Karo* establish

[79] *See Id.* at 515.
[80] *See Id.*
[81] *See Id.*
[82] *See Id.* at 517.
[83] *See* United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).
[84] *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 305 (3d Cir. 2010).

that "the privacy interests at issue are confined to the interior of the home."[85] Since the Third Circuit could find no evidence in the record that CSLI can implicate an individual's movements inside of his home, in their view, such information does not require a warrant.[86]

While it agrees with the Fifth and Eleventh Circuits that there is no need for a warrant, the Court differs in its analysis of the statutory language of the SCA. The Third Circuit came to a different conclusion than the Fifth Circuit on whether or not the statutory language gives the Court discretion when determining whether to issue such an order. The Court determined that if Congress wanted to require a mandatory disclosure of CSLI then they could have done so with the language "shall issue."[87] The Third Circuit reasons that the use of the language "'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence."[88]

The Third Circuit also departs from the analysis of the Fifth and Eleventh Circuits in concluding that CSLI is not voluntarily conveyed by users to service providers. In their view, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[89] Cell phone users only voluntarily convey to the service provider the number they dial and, in situations where they are receiving a call, they do not voluntarily convey anything.[90] While this language seems to suggest that the Third Circuit would consider a constitutional challenge to the statute, it ended its analysis with the familiar proposition that the legislature is the proper place for making such determinations.[91]

---

[85] *Id.* at 312.
[86] *See Id.* at 312-313.
[87] *See Id.* at 315.
[88] *Id.*
[89] In re United States for an Order, 620 F.3d at 317.
[90] *See Id.* at 317-18.
[91] *See Id.* at 319.

D. Sixth Circuit

In *United States v. Skinner*, decided in 2012, the defendant had come under suspicion of trafficking marijuana.[92] In order to track his movements, law enforcement would "ping" his phone allowing them to track his movements through CSLI.[93] This technique is different from the one which was utilized by law enforcement in the cases that reached the Third, Fifth, and Eleventh Circuits. In those cases, law enforcement was seeking to obtain historical CSLI that would show the defendants' movements over time.[94] In this case, the technique utilized by law enforcement allowed them to track the defendant's movements in real time by forcing his cell phone to record CSLI when it otherwise would not.[95] While this case does not regard an application of the government under the SCA, the Sixth Circuit nonetheless examines CSLI under the *Katz* framework.

The Court reasons that CSLI is the same as the information obtained from the beeper in *Knotts* and subject to the holding in that case that there was no reasonable expectation of privacy.[96] The Court contends that "while the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance," and as such there is no reasonable expectation of privacy.[97] The Court also emphasizes that the interests law enforcement have in tracking criminals outweigh the interests of cell phone users in having CSLI subjected to a warrant requirement when reaching their decision.[98]

---

[92] *See* United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012).
[93] *Id.* at 775-76.
[94] *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 305 (3d Cir. 2010); In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013); United States v. Davis, 785 F.3d 498, 502 (11th Cir. 2015).
[95] *See* Skinner, 690 F.3d at 776.
[96] *See Id.* at 778.
[97] *Id.*
[98] *See Id.* at 777.

Part IV. Circuits That Do Recognize a Reasonable Expectation of Privacy in CSLI

A. Fourth Circuit

While there are three circuits that decidedly state that CSLI does not receive the protections given by the Fourth Amendment, the Fourth Circuit is the only court to rule that it does receive such protections. The Fourth Circuit's ruling is the most recent, being rendered on August 5, 2015 in *United States v. Graham*. There, the defendant had participated in a string of robberies and the government obtained 221 days of CSLI, aiding in the conviction of the defendant.[99] The Court dismissed the defendant's claim that the CSLI evidence should not have been admitted at trial due to a clause in the defendants' contracts with their service providers noting the retention of CSLI and the possibility that the government might compel its disclosure. Nevertheless, the Court examined the constitutionality of obtaining CSLI without a warrant.[100]

The Court begins its analysis by noting that a search of historical CSLI is similar to the searches in *Karo* and *Kyllo* because the technology is precise enough to place a person inside of their home.[101] Moreover, the Court further reasons that CSLI is more invasive than the searches performed in *Karro* and *Kyllo* due to its constant transmission of information on the personal location as well as the length of time which the technology is utilized for.[102] In looking at the concurring opinions in *Jones*, the Court echoes the fears espoused in Justices Alito and Sotomayor's opinions. The Court fears that the constant monitoring of a person's location can be implicated through CSLI.[103] They reason that the technology is also more invasive than the GPS

[99] *See* United States v. Graham, 2015 U.S. App. LEXIS 13653, at *3-10 (4th Cir. 2015).
[100] *See Id.* at *21-22.
[101] *See Id*. at *24.
[102] *See Id*. at 25.
[103] *See Id*. at 28-29.

monitoring of an automobile since the cell phone is such an intimate item in modern society, capable of unveiling many aspects of a user's private life.[104] The Court concludes that "the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time."[105]

When faced with the contention that CSLI should be analyzed under the third party doctrine, the Court notes that CSLI is not voluntarily conveyed and thus is not applicable to be analyzed under the third party doctrine.[106] The Court reasons that because CSLI is generated without the user taking any affirmative process to create this information a user does not voluntarily convey CSLI.[107] The Court places an emphasis on the fact that CSLI can be generated by a user receiving a call or text message that they do not answer or respond to, highlighting their argument that CSLI is not conveyed by users to cell service providers.[108] They also refute the Fifth Circuit's analysis, which holds that users do voluntarily convey CSLI by deciding to use their cell phones, by arguing that "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones."[109] The Court concludes that an individual has a privacy interest in the aggregation of their movements over large periods of time and a service provider's retention of CSLI does not diminish that privacy interest.[110]

The Fourth Circuit finally considers the implications of the digital age on Fourth Amendment precedent. The Court notes that CSLI is unlike routing information, which has not been afforded Fourth Amendment protection, due to the fact that it conveys a user's location and

[104] *See* Graham, 2015 U.S. App. LEXIS 13653 at *30.
[105] *Id*. at *31.
[106] *See Id.* at *45-48.
[107] *See Id.* at *47-48.
[108] *See Id*. at *48.
[109] United States v. Graham, 2015 U.S. App. LEXIS 13653, at *50 (4th Cir. 2015).
[110] *See Id*. at *53-55.

there has been no evidence that users intend this information to be examined by others.[111] The Court posits that "even as technology evolves, protections against government intrusion should remain consistent with those privacy expectations society deems reasonable."[112] The Court notes that even though the advent of CSLI has left service providers with precise data on users' location information, this does not diminish the traditional societal expectation that individuals' movements would not be tracked and aggregated over lengthy periods of time.[113]

Part V. The Supreme Court Should Affirm Cell Phone User's Reasonable Expectation of Privacy in CSLI

While it may be the only circuit to hold that there is a reasonable expectation of privacy in CSLI, the Fourth Circuit's analysis of CSLI under the *Katz* framework is the proper one. CSLI is not a business record under the third party doctrine because cell phone users do not voluntarily convey this information to service providers. Cell phone users have a subjective expectation of privacy in CSLI and that expectation is objectively reasonable in society's eyes. CSLI is also precise enough to implicate the concerns expressed by Justices Alito and Sotomayor in their separate concurrences.

A. CSLI is Not a Business Record and Therefore Not Subject to the Third Party Doctrine

The Circuits, as well as scholars, have mainly focused their analysis under the third party doctrine around three factors: a general knowledge of how cell phones work, clauses in users' agreements alerting them to the retention of such information and the possibility that the

[111] *See Id.* at *58.
[112] *Id.* at *59.
[113] *See Id.* at *61-62.

government may compel its disclosure, and the voluntary nature of both cell phone use and CSLI generation.[114] These factors, however, do not prove that CSLI is a business record under the third party doctrine. A general knowledge of how cell phones work does not mean users have voluntarily conveyed their CSLI, and further users generally do not read their agreements in which clauses alerting them of this practice are contained. Cell phone use is also no longer voluntary for those who wish to fully participate in the modern economic and social society of America. Finally, the fact that CSLI is generated as an automatic byproduct of cell phone use further demonstrates that the third party business records doctrine is not applicable to CSLI.

As previously mentioned, some scholars rely on users' general understanding of cell phone technology as their support for the contention that users therefore understand what CSLI is and how it is generated.[115] "[W]hen a cell phone user makes or receives a call, and knows that his phone is communicating with the nearest cell tower, he is aware that he has conveyed his approximate location to the [cell service provider]."[116] This line of reasoning is seriously flawed because it assumes that users understand this technology. The United States Attorneys and the law enforcement agents themselves in most cases do not understand the technology and have a difficult time explaining it to the presiding judges when applying for a court order.[117] If sophisticated attorneys and law enforcement agents who work with this technology regularly cannot understand how it works, then it is hardly safe to assume that an average cell phone user

[114] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611-14 (5th Cir. 2013); Fraser, *supra* note 17, at 607-08; Fox, *supra* note 17, at 788-89 ("CSPs use it to determine roaming charges that appear on a subscriber's monthly statement. Thus, the roaming charges on the billing statement indicate to the subscriber that the physical location of the phone during a call is known and recorded by the subscriber's CSP in its regular course of business."); Malone, *supra* note 17, at 740 (2012).
[115] *See* Faser, *supra* note 17, at 607-08.
[116] *Id*.
[117] *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 40 (2013).

possesses such a level of understanding. Even if some users do possess such knowledge, this knowledge cannot be imputed to all cell phone users and to society as a whole.

Even assuming that users understand how cell phone technology works, it is hard to imagine average users being aware of the massive retention of this data for such lengthy periods of time.[118] Further, it is also unlikely that the average user understands how precise CSLI has grown as a result of the increase in competition amongst cell service providers to provide the best coverage. The improved precision of the location data as the distance between cell towers and their range shrink allows CSLI to track a person's whereabouts with increased accuracy.[119]

The Fifth Circuit also notes that users had voluntarily conveyed that information to the providers because they had agreed to the clause in the users' agreements that such information will be gathered and may be disclosed to the government. Thus, the clause demonstrates that they are records prepared in the ordinary course of business.[120] These provisions, however, are not routinely read nor are they understood by the users who sign up for these services.[121] "[C]ell phone users do not routinely scan the minutiae of their contract with the provider to find the buried provision relating to who owns the data or whether the service provider will release said data to law enforcement or any other third party."[122] Moreover, even if users are aware of the presence of these clauses, they have no meaningful option to negotiate for their removal or to choose a different provider, as these are standard clauses in nearly all service provider

[118] *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("[I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information.");] Babst, *supra* note 11, at 377 ("Most Americans have no idea that cell service providers store vast amounts of CSLI and allow the government warrantless access to it.").
[119] *See* United States v. Davis, 785 F.3d 498, 542 (11th Cir. 2015) (Martin, J., dissenting).
[120] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013).
[121] United States v. Graham, 2015 U.S. App. LEXIS 13653, at *20-21 (4th Cir. 2015).
[122] R. Craig Curtis et al., *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 90 (2014).

contracts.[123] It would be a mistake to entrust service providers with the task of safeguarding the privacy of their users' CSLI as profit motives will often lead to discounting user privacy concerns.[124] These clauses contained in users' contracts cannot serve as the basis for finding that CSLI are business records that were voluntarily conveyed.

The Fifth Circuit further reasons that the use of a cell phone is a voluntary action that the government does not compel and therefore CSLI is a business record subject to the third party doctrine.[125] The use of a cell phone is no longer as voluntary a choice as the Court likes to make it seem. As the statistics discussed earlier show, the use of cell phones is no longer confined to the more affluent segments of American society, but is utilized throughout all of American society.[126] For increasing segments of the American population cell phone ownership has become "essential to full cultural and economic participation."[127] Cell phone use has become a critical tool in performing occupational responsibilities and almost a social necessity in order to stay connected with friends and family.[128] This is especially true given the nature of the modern smartphone and all the functions it is capable of performing.[129] The contention that cell phone use is voluntary in American society is one that is detached from the reality of modern economic and social activity.

---

[123] *See* Megan L. McKewon, Note, *Who's Line is it Anyway?: Probable Cause and Historic Cell Site Data*, NOTRE DAME L. REV. 2039, 2056-57 (2015).
[124] *See* Babst, *supra* note 11, at 374.
[125] *See* In re Application of the United States, 724 F.3d at 613.
[126] *See Mobile Technology Fact Sheet*, PewInternet.org, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited October 3, 2015).
[127] United States v. Graham, 2015 U.S. App. LEXIS 13653, at *50 (4th Cir. 2015).
[128] *See* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH & LEE L. REV. 1745, 1786 (2009) ("Although many individuals choose to have cell phones for personal reasons, hoards of others are required to carry them for work, business, and other legitimate purposes.").
[129] *See* Christopher R. Orr, Note, *Your Digital Leash: The Interaction Cell Phone-Based GPS Technology and Privacy Rights in* United States v. Skinner, 45 U. TOL. L. REV. 377 (2014) ("Incorporating elements of traditional phones, personal organizers, and even computers, modern cell phones have features and capabilities that make them simultaneously indispensable and incomprehensible to those that employ them.").

Nearly every occupation now requires the ability to get in touch with colleagues and superiors at a moment's notice. To choose not to carry a cell phone will eliminate these individuals from certain occupations. For most of the American population this is no choice at all. Justice Marshall in his dissent in *Smith v. Maryland* made a similar argument about landline phone use and the contention that users had assumed the risk of the numbers they dialed being conveyed to law enforcement. He noted that "[u]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of assuming risks in contexts where, as a practical matter, individuals have no realistic alternative."[130] Cell phone users in modern society, as Justice Marshall observed of landline phone users, lack such a realistic alternative. As such, the third party doctrine has no relevance in analysis of CSLI.

It is also important to note that CSLI is generated without any affirmative act of the user. A user also lacks the ability to block the transmission of such information as well.[131] CSLI is generated not only when a user sends or receives a call or text message, but also when they receive a call or text message to which they do not answer.[132] This is even more so for smartphones which generate CSLI every time they receive "a push notification or download something in the background."[133] Consequently, such information cannot be said to be voluntarily conveyed by the user to the service provider. Even if cell phone users do not have an expectation of privacy when dialing phone numbers, it is a stretch to say that users are actively inputting their location before making a call.[134] Chamberlain sums up the issue when he states

[130] Smith v. Md., 442 U.S. at 749-50 (Marshall, J., dissent).
[131] *See* Graham, 2015 U.S. App. LEXIS 13653 at *46-48.
[132] *See Id*. at *48.
[133] Meyer, *supra* note 2.
[134] *See* United States v. Davis, 785 F.3d 498, 534 (11th Cir. 2015) (Martin, J., dissenting); *See* In re United States for an Order Directing Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-18 (3d Cir. 2010).

"CSLI is an automatic byproduct of cell phone use of which the average user is unaware. Individuals using cell phones, in other words, do not make an informed choice to allow their providers to record information about their movements."[135]

CSLI is also a far more intimate record than the bank records at issue in *Miller* or than the phone records at issue in *Smith* that were both deemed voluntarily conveyed business records.[136] In *Miller*, the records that law enforcement was able to obtain were "checks, deposit slips, two financial statements, and three monthly statements."[137] While these records certainly exposed intimate details about the defendant's life, they did not compile the in-depth picture of his daily activities that CSLI records can. Law enforcement may have learned that the defendant withdraw a sum of cash, but they would not have been able to see where he spent such cash and track his movements through these records. Similarly in *Smith*, all that law enforcement was able to obtain was a list of numbers the defendant had dialed.[138] While this information too was sensitive in nature, it did not paint an intimate picture of the defendant's life. All that was revealed by the pen register was the numbers he had dialed. It did not reveal the conversations he may have had in person or the places he may have visited without calling first. CSLI paints a far more intimate and detailed picture of an individual's life than either bank or landline phone records can. CSLI, like bank and landline phone records, is a snapshot of an instant in time, however, CSLI is generated to a far more frequent degree and is not confined to generation in certain locations like bank and landline phone records are. Additionally, when individuals conduct transactions with banks and use landline phones, they take clear, affirmative steps that create these records. CSLI,

[135] Chamberlain, *supra* note 128, at 1786.
[136] *See* United States v. Miller, 425 U.S. 435, 437-39 (1976); Smith v. Md., 442 U.S. 735, 737-38 (1979).
[137] Miller, 425 U.S. at 438.
[138] *See* Smith, 442 U.S. at 737.

however, is generated often without any affirmative action taken on behalf of the user, another indication that the third party doctrine is not applicable.

Since users do not have a detailed knowledge of how cell phone systems operate, they do not read or understand the clauses in service providers' contracts explaining the retention and possibility of compelled disclosure, cell phone use is no longer voluntary in today's society, and because CSLI is generated as an automatic byproduct, CSLI cannot be a business record under the third party doctrine. This finding then leads to analysis of cell phone users' subjective and objective expectations of privacy in CSLI in order to determine whether it deserves Fourth Amendment protections.

B. Cell Phone Users Have a Subjective Expectation of Privacy in CSLI

The Circuits and scholars who have argued that there is no reasonable expectation of privacy in CSLI have relied on the fact that it is a business record created during the ordinary course of business. Therefore, cell phone users do not have a subjective expectation of privacy. As discussed previously, CSLI is not a business record and thus requires an analysis under *Katz* of whether users have a subjective expectation of privacy.

It is difficult to imagine a user relinquishing their privacy interest in something they do not understand or even know exists.[139] Further, users do not have a choice in preventing CSLI from being generated, absent from abandoning the use of their cell phone. As such, users cannot be deemed to have given up their expectation of privacy. "People cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society

[139] *See* Orr, *supra* note 129, at 385 ("Subjectively, locational awareness in cell phones is not a feature that most people understand.").

through use of their cell phones."[140] It is hard to imagine that in "a nation founded on the principles of liberty and freedom [a] . . . pre-condition for participation in the social and business life of the nation is to give to the government the ability to track your location at all times."[141] As the Fourth Circuit aptly reasons "[i]n the absence of any evidence that . . . cell phone users generally intend for their location information to be open to inspection by others" there can be no other conclusion than that users retain a subjective expectation of privacy in their CSLI.[142]

Some scholars point to the fact that some applications on smartphones contain features that allow users to share their location as an indication that users have given up their subjective expectation of privacy in their location data.[143] This confuses the issue, as the information shared in applications is not the same as CSLI. This type of location information is not information that is continuously generated throughout the day without the user's affirmative actions. When users share their location to their friends and family on social media or other location based apps, it is for a single moment in time. This selective, single-instant sharing of location cannot be assumed to be a signal from users that they relinquish all privacy rights that they may have in any location information generated from the use of their cell phone.

Since CSLI is not a business record under the third party doctrine, the contention that users do not have a subjective expectation of privacy cannot be justified under this theory. Most users do not understand how the technology works and have no capability to stop the information from being generated. Thus, users have a subjective expectation of privacy in CSLI.

---

[140] United States v. Graham, 2015 U.S. App. LEXIS 13653, at *50 (4th Cir. 2015).
[141] Curtis, *supra* note 122, at 91.
[142] Graham, 2015 U.S. App. LEXIS 13653 at *58.
[143] *See* Malone, *supra* note 17, at 733 ("Google Latitude is just one of many applications that, if someone chooses, will display her location on a map for all of her chosen friends to see either on their smartphone devices or computer. Someone utilizing an application such as this cannot claim any subjective expectation of privacy").

C. Users Have an Objective Expectation of Privacy

It is important to remember at the outset of the objective portion of the *Katz* analysis that "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[144] This reasonable person test is largely dependent upon a judge's own personal construction when faced with an order to compel such disclosure or upon appellate review and can change in the face of advancing technology.[145] Most judges do not have a "technological expertise," which may also contribute to a judge's substitution of society's reasonable expectations with that of the experts in the field writing amicus briefs who may have their own agendas.[146] In his concurrence in *Jones*, Justice Alito correctly reasoned that "society's expectation has been that law enforcement agents and others would not – and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual."[147] While Justice Alito was speaking about GPS monitoring, the same could be said for the use of CSLI.

"Recent polling data tells us that 82% of adults feel as though the details of their physical location gathered over a period of time is very sensitive or somewhat sensitive."[148] This number accurately reflects the notion that a reasonable person expects their CSLI to remain private. Society has long recognized a reasonable expectation of privacy in their phone conversations. Simply because their phones now have the ability to monitor their location as well does not mean that users do not expect government to obtain a warrant before doing so.[149] The advent of this new technology has made it capable to track people's movements over lengthy periods of time.

[144] United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).
[145] *See* Curtis, *supra* note 122, at 77-78.
[146] *See* Orr, *supra* note 129, at 395-96.
[147] United States v. Jones, 132 S. Ct. at 964 (Alito, J., concurring).
[148] United States v. Davis, 785 F.3d 498, 538 (11th Cir. 2015) (Martin, J., dissenting).
[149] *See* Babst, *supra* note 11, at 377-78; Fraser, *supra* note 17, at 603-04.

Society does not expect that a person can be tracked in such a discrete manner and without the expenditure of large amounts of law enforcement resources. Simply because it is now possible to track a person using cell phone towers, that reasonable expectation should not change.[150]

As the Fourth Circuit holds, the Supreme Court precedent leads to the conclusion that "the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time."[151] It has been recognized that a person has a privacy interest in their movements over time and their movements in their home, CSLI technology has the capability to, and often does, invade those traditionally recognized areas of privacy.[152] Merely because new technology has given law enforcement new methods in their pursuit of criminals does not mean traditionally held expectations of privacy are abrogated. The *Katz* doctrine has adapted to new technology in *Knotts* and *Karro*, *Kyllo*, and *Jones* and it needs to do so again in the face of compelled disclosure of CSLI.[153]

Some scholars have suggested that if *Katz* could be "taken to its logical conclusion" then the government could simply announce that they are using such technology to erase any reasonable expectation of privacy in CSLI.[154] This argument is incorrect, as nothing that the government "announces" can diminish society's reasonable expectations of privacy that have long been recognized in traditional places such as the home. Widespread knowledge of an objectively viewed unlawful governmental activity can never diminish reasonable expectations of privacy. "[N]ot recognizing an expectation of privacy when one knows that their privacy can

[150] United States v. Graham, 2015 U.S. App. LEXIS 13653, at *61-62 (4th Cir. 2015).
[151] *Id.* at *31.
[152] *See Id.* at *54.
[153] *See* United States v. Knotts, 460 U.S. 276, 278 (1983); Kyllo v. United States, 533 U.S. 27, 29-30 (2001); United States v. Jones, 132 S. Ct. 945, 948 (2012).
[154] *See* Fraser, Comment, *supra* note 17, at 603-04.

be infringed upon will eventually result in no privacy expectations as technology becomes more invasive."[155] The reasonable expectation of privacy will only continue to grow, not diminish, as this technology becomes more and more precise and smartphone ownership grows.[156]

Cell phone users have a reasonable expectation of privacy in CSLI because it implicates areas that have traditionally been recognized as having privacy rights and users widely regard their location information as being sensitive. That new technology allows law enforcement to do things that were previously unimaginable does not mean we need to reimagine our expectations of privacy that have been traditionally held and respected by government.

D. CSLI is Precise Enough to Implicate Jones' *Concurrence Concerns as Well as Traditional Privacy Rights in the Home*

Justice Alito in his concurrence in *Jones* acknowledges that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[157] CSLI monitoring, while not as precise as GPS in every instance, has the capability of being just as invasive, if not more so, than GPS monitoring of a person's movements. CSLI also has the ability to track users in locations that GPS devices previously could not.[158] The proliferation of cell towers has made the "antennas, microcells, and femtocells" capable of "reveal[ing] . . . location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot."[159] The Supreme Court itself has recently recognized the ability of CSLI to

---

[155] Matthew Devoy Jones, Note, *The "Orwellian Consequence" of Smartphone Tracking: Why a Warrant Under the Fourth Amendment is Required Prior to the Collection of GPS Data*, 62 CLEV. ST. L. REV. 211, 236 (2014).
[156] *See* P. Kramer Rice, *You Are Here: Tracking Around the Fourth Amendment to Protect Smartphone Geolocation Information with the GPS Act*, 38 SETON HALL LEGIS. J. 17, 33 (2013).
[157] United States v. Jones, 132 S. Ct. at 964 (Alito, J., concurring).
[158] Babst, *supra* note 11, at 376 ("New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers.").
[159] United States v. Davis, 785 F.3d 498, 542 (11th Cir. 2015) (Martin, J., dissenting).

"reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." [160]

Simply because there are sparsely populated areas with few cell phone towers where this technology is utilized, the opposite scenario of densely populated areas with a multitude of cell phone towers cannot be immediately discounted. It is undeniable that a vast percentage of cell phone users live in densely populated areas where cell towers are most needed to provide users with a service capable of handling the massive amount of daily activity. While some circuits and scholars may tend to discount this fact, the reality is for many Americans living in urban environments the tracking of CSLI has become precise enough to be relied on in the same manner that GPS technology is.[161]

As the Fourth Circuit has argued, CSLI may provide a more intimate picture of a user's life than GPS monitoring of a car, in that while a person is not moving at all times in his car, he or she is rarely without his or her cell phone.[162] This would allow the government to track an individual in their movements "between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home."[163] This type of tracking surely implicates greater privacy interests than the GPS monitoring of a person's car does, especially when viewed over a longer period of time. As cell phone technology improves and the amount and density of cell towers continue to grow, CSLI will only grow more precise, not less, further indicating that it is, or if it is not now it shortly will be, analogous to GPS technology.[164] Even if it is accepted that CSLI is not currently as precise as GPS technology, it

[160] Riley v. California, 134 S. Ct. 2473, 2490 (2014).
[161] *See* United States v. Graham, 2015 U.S. App. LEXIS 13653, at *28 ("Much like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life.").
[162] *See Id*. at *29.
[163] *Id*.
[164] *See* McKewon, *supra* note 123, at 2057-58.

still reveals location information with an "unnerving level of specificity" implicating *Jones* concerns.[165]

The purpose for which law enforcement uses this information is another indication that CSLI implicates *Jones* concerns. "The general character of cell site location information and the purposes for which the government seeks it make it largely analogous to GPS location information."[166] The government is not seeking this information for purposes other than to identify where the defendant was at a precise moment in time. Rather, the government is aggregating this information to make it more likely that the defendant is guilty of what the government is accusing him or her of. While law enforcement should not be prohibited from utilizing new technology, they should simply be required to show probable cause before being allowed to access information that reveals such intimate details of an individual's life. Even though it currently may not be as precise as GPS monitoring, "it is far more ubiquitous, because every cell phone is capable of being located by CSLI technology."[167] Law enforcement will not have to go through the trouble of placing a GPS device on a person or their car; instead, they will merely utilize what in effect is a GPS device that users have voluntarily placed on themselves.[168] This will make it far easier for law enforcement to utilize and, in turn, to abuse this technology.

CSLI is also precise enough to implicate the long recognized privacy right of the home. The Court in *Kyllo* stated a search has occurred if information is obtained regarding the interior of the home through technology not in general use.[169] In that case thermal vision, which was not

---

[165] United States v. Davis, 785 F.3d 498, 540 (11th Cir. 2015) (Martin, J., dissenting).
[166] *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 630 (5th Cir. 2013) (Dennis, J., dissenting).
[167] Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 239 (2012).
[168] *See* Jones, *supra* note 155, at 235 ("[W]henever individuals are carrying their smartphone on their person in public, the government may legally follow their every move without a warrant.").
[169] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

in general public use, was utilized to discern details about the interior of the home.[170] The modern counterpart of this technology has now become CSLI. Like thermal vision, while it may not operate like x-ray vision allowing law enforcement to literally see through the wall of a home, CSLI still allows law enforcement to uncover details about the interior of the home that they could not have uncovered through mere visual surveillance. Moreover, it is clear that the computer programs being utilized by the government to analyze and plot CSLI are not currently in general use. Even if analogized as GPS information, it can hardly be said that users of that technology have ready access to obtain GPS information about other users.[171] "There is no widely available program . . . for utilizing GPS data," it requires highly technical skills and programs not possessed by the public.[172] The general public's utilization of GPS technology is to find out information about their own location, not location information about other users. To claim that even GPS technology, as utilized by the government in *Jones*, is technology available to the public would strain credulity.

In *Graham*, the government collected an average of 100 data points per day on each defendant, leading to the Fourth Circuit to argue that surely some of these data points indicated that the defendants were at their home.[173] As was stated in *Kyllo*, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained . . . In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[174] It is not determinative to say that CSLI cannot track a user's movements from one room of their house to another. If a person's presence

[170] *See Id.*
[171] *See* Orr, *supra* note 129, at 388.
[172] *Id*.
[173] *See* United States v. Graham, 2015 U.S. App. LEXIS 13653, at *35 (4th Cir. 2015).
[174] Kyllo, 533 U.S. at 37.

in his home could not be observed through visual surveillance, the use of CSLI to find out this information clearly violates a traditional expectation of privacy. This is especially true because law enforcement cannot know which location points will be uncovered when the CSLI is disclosed, making the search presumptively unconstitutional.[175] That is why it is no solution to require as a "threshold determination," as some have suggested, to have the magistrate assess whether the CSLI will implicate a user's presence in their home before they may grant such an order.[176] It will be impossible for magistrate judges to make such a determination before the disclosure occurs without guessing about a user's daily habits or after being presented with information by law enforcement officials regarding visual observations of a user's movements, effectively rendering CSLI duplicative.

CSLI is also implicated by Justice Alito's concurrence in *Jones* by the fact that it has the capability of revealing a person's movements while in private spaces. With the prevalence of cell phone use it is likely that one of the many location points uncovered will locate a person inside of their home. In rare cases involving large residences, it may even be possible to achieve this precision in tracking an individual from room to room. "Although examples involving sprawling but private locations of this sort admittedly are exceptional cases, even exceptional cases undermine the opponents' position that CSLI never can reveal more than that which can be observed by visual surveillance."[177] The ability of CSLI to locate a cell phone user inside their residence is also reason to reject the argument that a durational requirement on court orders

[175] *See* Jones, *supra* note 155, at 235-236; Chamberlain, *supra* note 128, at 1787 ("[T]he practical reality is that [service providers] are unable to filter their CSLI according to the type of location it reveals.").
[176] Steven M. Hawkins, Note, *CSLI Disclosure: Why Probable Cause is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH & LEE L. REV. 1875, 1918 (2011) ("In order to answer this question in the negative, a reviewing magistrate judge would have to decide that automatic cell phone registration, which takes place approximately every seven seconds, would not place the target within the home at any point during the period for which disclosure is requested.").
[177] Chamberlain, *supra* note 128, at 1788.

compelling CSLI can cure Fourth Amendment concerns.[178] A user's presence in his residence could be observed in a single day's CSLI, violating the Fourth Amendment.

The Court in *Karo* similarly recognized that although law enforcement had followed the signal from the beeper to the residence lawfully, once they were able to discern that it was inside the house, something they would not have been able to observe visually, a search had occurred.[179] Similarly with CSLI, law enforcement could observe a person enter their home, but then fail to observe the same individual leave through another entrance not known to them. If CSLI continues to show the individual in their home for elongated periods of time, law enforcement is able to learn something that they would not normally be able to without a warrant.[180] The Court in *Karo* could not accept the argument that law enforcement should be free of the requirements of the Fourth Amendment when "determin[ing] by means of an electronic device, without a warrant . . . whether a particular article – or a person, for that matter – is in an individual's home at a particular time."[181] This same reasoning is applicable to CSLI, which is precise enough to determine whether a person is in their house at a particular time.

CSLI technology implicates the concerns raised in Justice Alito's concurrence in *Jones* because it is precise enough and used for the same purposes in order to analogize it to the use of GPS technology. Similarly to GPS technology, it can also reveal a person's movements in private spaces, which has been constitutionally recognized as a private place.

Part VI Conclusion

[178] *See* Jones, *supra* note 155, at 242.
[179] *See* United States v. Karo, 468 U.S. 705, 713-15 (1984).
[180] *See Id.* at 715 ("Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises."
[181] *Id.* at 716.

It is no longer science fiction to think that the government has the capability of tracking a person's every movement without a warrant; they possess this capability through examination of a cell phone user's CSLI. It is evident that with the differing circuit opinions, both law enforcement and judges tasked with hearing these requests lack clarity on what the current state of the law is.[182] This lack of clarity is exacerbated by the portable nature of cell phones and their ability to cross not only state boundaries, but circuit court boundaries as well.[183] The Supreme Court would be well advised to weigh in on this growing field of controversy amongst the circuit courts.

When the Supreme Court does hear a question on CSLI, it will be clear that the Fourth Circuit's analysis of CSLI under the *Katz* test is the correct one. This comment has examined the Supreme Court precedent under *Katz* as well as analyzed each Circuit Court's opinion that has addressed this issue. CSLI cannot be a business record due to the fact that a user does not voluntarily convey this information to a cell service provider. Thus, the third party doctrine is inapplicable to CSLI. Looking at expectations of privacy, cell phone users have a subjective expectation of privacy in CSLI because most do not understand the technology and when asked about the privacy of their location information cell phone users overwhelmingly respond that they consider such information to be private. Cell phone users' expectation of privacy is also objectively reasonable in society's eyes because the aggregation of a person's movements as well as the invasion of a private space have all been traditionally afforded privacy protections and CSLI is capable of implicating both of these privacy concerns.

[182] *See* Curtis, *supra* note 122, at 89.
[183] *See* Elizabeth Elliott, United States v. Jones*: The (Hopefully Temporary) Derailment of Cell-Site Location Information Protection*, 15 Loy. J. Pub. Int. L. 1, 35 (2013).

Although opponents of a probable cause standard for CSLI might harp on the difficulty this would create for law enforcement to carry out their responsibilities, all this comment proposes is merely that law enforcement seek a warrant before examining such information. This would not cripple law enforcement's efforts to catch criminals; it would only safeguard society's privacy. This is an entirely reasonable requirement in light of the pervasiveness of the cell phone in today's modern society. As Justice Marshall stated "[p]rivacy . . . . is of value not only to those engaged in criminal activity. The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide."[184]

[184] Smith v. Md., 442 U.S. at 751 (Marshall, J., dissent).