Cell Phone or Government Tracking Device?: Protecting Cell Site Location Information with Probable Cause

Samantha G. Zimmer

Follow this and additional works at: https://dsc.duq.edu/dlr

Part of the Communications Law Commons

Recommended Citation
Available at: https://dsc.duq.edu/dlr/vol56/iss1/7

This Student Article is brought to you for free and open access by Duquesne Scholarship Collection. It has been accepted for inclusion in Duquesne Law Review by an authorized editor of Duquesne Scholarship Collection.
Cell Phone or Government Tracking Device?  
Protecting Cell Site Location Information with Probable Cause

Samantha G. Zimmer*

I. INTRODUCTION..........................................................107
II. CSLI AND THE STORED COMMUNICATIONS ACT ..........110
III. PATCHWORK OF PRECEDENT.....................................112  
    A. Reasonable Expectation of Privacy and the  
       Third-Party Doctrine .........................................113
    B. The Mosaic Theory and Location Tracking  
       Devices .............................................................115
IV. CIRCUIT SPLIT AND REALIGNMENT .........................119  
    A. Eleventh Circuit Approach ..............................120
    B. Sixth Circuit Approach .................................121
    C. Fourth Circuit Approach .................................123
V. ARGUMENT................................................................125  
    A. Insufficiency of the Third-Party Doctrine  
       and Mosaic Theory ..............................................126
    B. The Solution: A Blend of the Judiciary and  
       the Legislature ..................................................130  
       1. Overruling the Third-Party Doctrine  
          in Carpenter ....................................................130
       2. Congressional Action: Requiring  
          Probable Cause .................................................136
VI. CONCLUSION.............................................................139

I. INTRODUCTION

Assume it is Saturday morning, and you wake up and check your cell phone. You text your friend on your walk to brunch, and post a photo of your waffle on Instagram while there. Afterwards, you call your family as you drive to the pharmacy, where you check your

* Samantha G. Zimmer is a 2018 J.D. candidate at Duquesne University School of Law. She graduated from the Pennsylvania State University in 2015 with B.A. degrees in Comparative Literature and Telecommunications with highest honors.
email while you are in line. All in these few hours, your phone has connected to cell towers\(^1\) close to you as you move, even crossing into cells created by different towers as you travel. Each time you begin one of these activities, you connect to your cell phone carrier’s network.

The average cell phone user connects to the cell phone carrier’s network countless times a day, whether the user is cognizant of it or not.\(^2\) When calls are placed, text messages are sent, or pictures are posted to social media, the phone connects to the network via a nearby cell tower.\(^3\) When this happens, information relating to this network connection is collected by cell phone carriers as part of routine business practices.\(^4\) This information that is generated and recorded by the carriers (“Cell Site Location Information” or “CSLI”) contains not only an approximation of the location of the phone, but also information about date and time of calls, duration of calls, and to whom calls are placed.\(^5\) CSLI is highly prolific, as is evidenced by Timothy Carpenter, whose case is about to come before the Supreme Court. Carpenter connected to his carrier’s network so many times over the course of 127 days that it created 12,898 data points regarding his cell site location.\(^6\) Under the current law, law enforcement officers were able to obtain this significant amount of sensitive information without probable cause.\(^7\)

Timothy Carpenter’s case is not unusual. As the presence of technology increases rapidly, personal information about users becomes less private.\(^8\) But in a world where technology changes almost daily and laws remain stagnant for decades, courts and legislatures are tasked with finding the delicate balance between outdated laws, and...
technological advancement, and personal liberties. The Fourth Amendment has become the center of this balancing act, as the right to be free from unreasonable searches and seizures is analyzed in this new light. With the advancement of technology leading to the proliferation of cell phones, many law enforcement agencies seek CSLI when gathering evidence in a criminal investigation. Warrantless acquisition of CSLI by law enforcement officers from cell phone carriers presents one example of the increasing tension between government interests and individual privacy in the technological age.

CSLI searches hang in the balance of this tension with courts coming to different conclusions about the amount of protection CSLI should receive under the Fourth Amendment. Some courts have relied upon the third-party doctrine, finding that individuals lose a reasonable expectation of privacy in CSLI since it is voluntarily conveyed to the carrier. Some courts have rejected the third-party doctrine, alternatively finding that this information is

9. Laurie Buchan Serafino, "I know my rights, so you go'n need a warrant for that": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third Party Clouds, 19 BERKELEY J. CRIM. L. 154, 156 (2014).
10. U.S. CONST. amend. IV. Specifically, the Fourth Amendment states that: [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
11. Reitmayer, supra note 8, at 99.
12. See Annual Wireless Industry Survey, CTIA, http://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey (last visited Jan. 13, 2017). In a recent survey of cell phone usage, it was found that there were 377.9 million wireless subscriber connections. Id. Additionally, the wireless penetration rate (the number of active wireless units divided by the total United States population) was 115.7%. Id.
15. See generally United States v. Davis, 785 F.3d 498 (11th Cir. 2015). The third-party doctrine establishes that an individual has no reasonable expectation of privacy in "information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
not conveyed voluntarily. As a result, those courts have held that gathering CSLI is a Fourth Amendment search, because users have a reasonable expectation of privacy. Still other courts have avoided the third-party doctrine in relation to location data, favoring instead an analysis of the prolonged search on the whole under what is termed as the mosaic theory.

Courts will remain divided on the issue of CSLI until some action is taken by both the Supreme Court and Congress to clarify this ambiguous area with its varied doctrines and precedent. Under current law, there are no sufficient solutions. The established Fourth Amendment jurisprudence is insufficient to cover the unique nature of CSLI. Additionally, the third-party doctrine is impractical applied to modern technologies, and the mosaic theory poses more questions than answers. The recent split in circuit courts of appeal on this issue demonstrates that the courts alone are not the proper vehicle through which to increase CSLI search and seizure protection. The Supreme Court is now posed to finally take on the issue on appeal in United States v. Carpenter, but the solution cannot begin and end there. In order to ensure Fourth Amendment protection for CSLI, the Supreme Court should limit continued application of the third-party doctrine in the technological context, specifically as applied to CSLI, as third-parties are inescapable in modern communications. Additionally, Congress should enact a comprehensive statute codifying the requirement of a warrant based on probable cause prior to the government’s acquisition of any CSLI.

II. CSLI AND THE STORED COMMUNICATIONS ACT

When cell phones are turned on, they connect to network cell towers via specifically assigned network and cell phone identification

16. See, e.g., United States v. Graham (Graham 1), 796 F.3d 332 (4th Cir. 2015), vacated, 824 F.3d 421 (Graham 1) (4th Cir. 2016); In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1031, 1033, 1035 (N.D. Cal. 2015).
numbers.\textsuperscript{20} Depending on the location of the phone among the towers, the network then decides though which tower to route the call.\textsuperscript{21} The cell phone continues to send information about the location of the phone in relation to the tower periodically to the carrier while the phone is turned on and connecting to the network.\textsuperscript{22} When the phone is in an area with more towers, the location of the phone can be more precisely pinpointed.\textsuperscript{23} CSLI can be either historical, meaning law enforcement receives the records after the fact, or real-time, where law enforcement can track the suspect’s location movement as it is occurring.\textsuperscript{24} For the purposes of this article, CSLI will refer to both real time and historical.\textsuperscript{25}

Law enforcement can obtain a suspect’s CSLI under the procedures set forth in the Stored Communications Act ("SCA").\textsuperscript{26} Passed over twenty years ago, the SCA is tailored to an older era of technology and focuses on the distinction between content and non-content\textsuperscript{27} when determining what level of protection certain information receives.\textsuperscript{28} Specifically, under the SCA, there are certain requirements for obtaining "contents of a wire or electronic communication"\textsuperscript{29} that differ from non-content.\textsuperscript{30} Non-content is considered "a record or other information pertaining to a subscriber or to a customer of such service (not including the content of communications)."\textsuperscript{31} For non-content information under the SCA, the government can require a "provider of electronic communication service . . . to disclose a record" after a law enforcement officer obtains a court order.\textsuperscript{32} The request for the order does not require probable cause, but rather just "specific and articulable facts showing that

\begin{itemize}
\item \textsuperscript{20} Brian et al., \textit{supra} note 1. Cell Phones have various codes associated with them for network verification. \textit{Id.} When the cell phone is turned on, the network verifies the user through a system identification code unique to the carrier, as well as an electronic serial number unique to the individual phone. \textit{Id.}
\item \textsuperscript{21} Harkins, \textit{supra} note 3, at 1882.
\item \textsuperscript{22} \textit{Id.} at 1881-82.
\item \textsuperscript{23} \textit{Id.} at 1883.
\item \textsuperscript{24} Corbett, \textit{supra} note 4, at 217.
\item \textsuperscript{25} For this article, the distinction between real-time and historical CSLI does not factor into the argument or analysis for increased Fourth Amendment protection. Rather, it is argued that all CSLI should be given full protection under the Fourth Amendment regardless of whether it is collected by a third party or the government.
\item \textsuperscript{26} See generally 18 U.S.C.A §§ 2701-2712 (West 2016).
\item \textsuperscript{27} \textit{Id.} § 2703(a).
\item \textsuperscript{28} Corbett, \textit{supra} note 4, at 218.
\item \textsuperscript{29} 18 U.S.C.A. § 2703(a) (West 2016).
\item \textsuperscript{30} \textit{Id.} § 2703(b).
\item \textsuperscript{31} \textit{Id.} § 2703(c).
\item \textsuperscript{32} \textit{Id.}
there are reasonable grounds to believe [the records] are relevant and material to an ongoing criminal investigation.”

The SCA requires that the records provided pursuant to the Act contain various types of information, including the length of call and service. However, the SCA does not specify location information as something that must be on the disclosed records. Despite the fact that the SCA is silent with regards to location information, CSLI has been classified by law enforcement and courts as non-content information that falls under the less strict proof standard of the SCA. It is this standard of less than probable cause that has been at the center of appeals focused upon greater Fourth Amendment protection for CSLI.

III. PATCHWORK OF PRECEDENT

The SCA is the statutory provision law enforcement utilizes to obtain CSLI. However, because the SCA does not specifically contemplate this type of information, litigants are raising the issue of whether CSLI collection is a Fourth Amendment search. A recent movement in courts acknowledges the need for increased protection of the copious information mined from technology. Yet, the controlling precedent still focuses on specific or outdated technology in limited circumstances.

33. Id. § 2703(d). Under the provisions of the SCA regarding content of communications, the government may only compel disclosure of content of communications after obtaining a warrant based on probable cause or with prior notice to the subscriber and an administrative subpoena or court order. Id. § 2703(b).
34. Id. § 2703(c)(2).
35. Id. The SCA enumerates that the record holder shall disclose the: name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity . . . and means and sources of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service. Id.
36. Id. § 2703(d).
37. See generally Graham I, 796 F.3d 332 (4th Cir. 2015); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2015).
38. Compare Riley v. California, 134 S. Ct. 2473, 2489 (2014) (acknowledging cell phones collect distinct, revealing information that warrants greater protection), with United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2015) (comparing CSLI to information found on the outside of a mailing, which is not constitutionally protected).
A. Reasonable Expectation of Privacy and the Third-Party Doctrine

The Supreme Court has not yet addressed the issue of what, if any, Fourth Amendment protection is awarded to CSLI. Therefore, the Court’s established Fourth Amendment jurisprudence is the only guidance for lower courts facing this issue. 40 Although trespass principals defined early Fourth Amendment analyses, the modern Fourth Amendment construction is largely premised on the concept that the Fourth Amendment “protects people, not places.” 41 As such, the Fourth Amendment analysis focuses on whether an individual has both a subjectively and objectively reasonable expectation of privacy that is violated by a particular search. 42 This analysis, termed the Katz test, is two-pronged. 43 First, courts determine whether an individual has an actual expectation of privacy. 44 Second, if the individual does have an actual expectation of privacy, courts determine whether that expectation is “one that society is prepared to recognize as ‘reasonable.’” 45

The Supreme Court first looked to Fourth Amendment reasonable expectations of privacy in relation to telecommunications in 1979 in Smith v. Maryland, where it brought the established third-party doctrine into an age of technology. 46 In Smith, the police, without a warrant, installed a pen register 47 on a telephone company’s equipment to record the phone numbers dialed from the defendant’s landline phone. 48 The Court held that there was no reasonable subjective expectation of privacy for telephone users when it came to numbers dialed on the phone. 49 This was because such information must be conveyed to the telephone company, a third party, as part of the transaction. 50 Further, even if the defendant

41. Katz v. United States, 399 U.S. 347, 351 (1967); See also Jones, 132 S. Ct. 949 (emphasizing that the history of the Fourth Amendment is closely connected to the principles of property and trespass).
42. Katz, 399 U.S. 361 (Harlan, J., concurring).
43. Id.
44. Id.
45. Id.
47. The pen register was not a listening device for wiretapping purposes, but instead recorded the telephone numbers dialed from a suspect’s home phone. Id. at 737.
48. Id.
49. Id. at 743.
50. Id.
did have a subjective expectation of privacy, there was no reasonable objective expectation that this information would be private.\textsuperscript{51} In noting this, the Court harkened back to the established third-party doctrine, whereby an individual does not have a reasonable expectation of privacy in information voluntarily given to third parties.\textsuperscript{52} Thus, since the defendant “voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record . . . [the defendant] assumed the risk that the information would be divulged to police.”\textsuperscript{53}

Many of the twenty-first century concerns about the third-party doctrine, including assumption of the risk and lack of technology alternatives, were present when \textit{Smith} was decided.\textsuperscript{54} Justice Marshall dissented from the majority in \textit{Smith}, presenting some of the first arguments as to the possible shortcomings of the third-party doctrine when applied to technology.\textsuperscript{55} Marshall was skeptical of the majority’s assumption that individuals are generally aware that the information they convey to phone companies is recorded and compiled as part of business records.\textsuperscript{56} Additionally, Marshall argued against the majority’s reliance upon the consumer’s assumption of the risk of disclosure under the third-party doctrine.\textsuperscript{57} He advocated that it was unfair to claim assumption of the risk when there was no practical alternative to using the phone.\textsuperscript{58} The only alternative to avoid this possible disclosure was to “forgo use of what for many has become a personal or professional necessity.”\textsuperscript{59}

Marshall argued instead that the test for a reasonable expectation of privacy under \textit{Katz} should be dependent on the risks an individual “should be forced to assume in a free and open society.”\textsuperscript{60} Thus, Marshall would have held that there is a reasonable expectation of privacy in phone numbers dialed, and that law enforcement

\textsuperscript{51} Id. at 743-44.
\textsuperscript{52} Id. at 743-44; see, e.g., United States v. Miller, 425 U.S. 435, 443 (1976) (noting that in terms of banking information, “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party”); Couch v. United States, 409 U.S. 322, 335 (1973) (finding there to be no expectation of privacy in records given to an accountant).
\textsuperscript{53} Smith, 442 U.S. at 745.
\textsuperscript{54} See generally id. at 749-50 (Marshall, J., dissenting).
\textsuperscript{55} Id. at 748-49. As will be discussed later, Justice Stewart dissented separately from the \textit{Smith} majority, presenting the first sentiments that would come to resemble the mosaic theory. Id. at 748 (Stewart, J., dissenting).
\textsuperscript{56} Id. at 749 (Marshall, J., dissenting).
\textsuperscript{57} Id.
\textsuperscript{58} Id. at 750.
\textsuperscript{59} Id.
\textsuperscript{60} Id.
officers should be required to obtain warrants prior to asking a telephone company to disclose such information. Nevertheless, despite the concerns voiced by Justice Marshall, the third-party doctrine prevails and constitutes the primary standard under which courts determine that technological information does not have full Fourth Amendment protection.

B. The Mosaic Theory and Location Tracking Devices

As Fourth Amendment jurisprudence has developed along with technological advancements, the mosaic theory has emerged as a possible replacement to the third-party doctrine. While something similar to the mosaic theory appeared in Justice Stewart’s dissenting opinion in *Smith v. Maryland*, the modern mosaic theory is largely credited to the District of Columbia Circuit Court of Appeals in the case of *United States v. Maynard*. In *Maynard*, the police attached a GPS tracking device to the defendant’s jeep without a warrant and tracked his movements with the device for approximately a month. The Circuit Court found the *Maynard* case to present an issue typically left unanswered by past precedent: “whether ‘wholesale’ or ‘mass’ surveillance of an individual requires a warrant.” After finding that the attachment of a GPS tracking device did constitute a search under the Fourth Amendment, the court applied *Katz* and found the defendant had a reasonable expectation of privacy in the whole of his movements.

The court used *Smith* to support this interpretation of the Fourth Amendment, noting that the *Smith* Court’s analysis was focused not only on a reasonable expectation of privacy in the numbers dialed, but also on a reasonable expectation that the numbers dialed would be compiled in a list. As a result, the reasonable expectation of privacy was composed of “parts” (the numbers dialed) that make up the “whole” (the compiled list of the numbers dialed).

61. Id. at 752.
62. Serafino, supra note 9, at 168.
63. Kerr, supra note 18, at 313.
64. Smith, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting) (noting the information from the pen register should be protected not because it could be incriminating, but because the information taken together shows the people and places called, thus revealing “the most intimate details of a person’s life”).
66. Id. at 555.
67. Id. at 558.
68. Id. at 560.
69. Id. at 561.
70. Id.
The D.C. Circuit Court then reasoned that the privacy interest in the whole could be greater than the privacy interests in the parts.\textsuperscript{71} The concept of the mosaic theory by the Maynard court suggests that the prolonged search of an individual's location compiled on the whole reveals a more detailed picture of a person's life than one piece of tracking information alone.\textsuperscript{72} Consequently, there is an objectively reasonable expectation of privacy in society for such a search.\textsuperscript{73} For example, the court notes that while location data showing a visit to the gynecologist is not particularly revealing on its own, that snippet of location information coupled with data indicating another location to be a trip to a baby supply store is indeed revealing.\textsuperscript{74}

On appeal, in the consolidated case \textit{United States v. Jones}, the Supreme Court affirmed the D.C. Circuit Court, finding that the GPS tracking did constitute a search of a protected area under the Fourth Amendment.\textsuperscript{75} However, the Court declined to apply the \textit{Katz} reasonableness analysis or the D.C. Circuit's mosaic theory, and applied traditional trespass principles instead.\textsuperscript{76} The Court noted that \textit{Katz} did not "narrow the Fourth Amendment's scope," thus, the traditional property and trespass principles of the Fourth Amendment remained and were sufficient to settle the dispute in this case.\textsuperscript{77} As a result, the warrantless attachment of the GPS to the car was an intrusion on a constitutionally protected area that violated the Fourth Amendment.\textsuperscript{78}

The \textit{Jones} opinion is perhaps most interesting in the evolving Fourth Amendment jurisprudence because of the concurring opinions presented.\textsuperscript{79} Although the Court chose not to give weight to the mosaic theory analysis utilized by the D.C. Circuit, Justice Sotomayor expressed some support for the theory in her concurrence, as technological advances make non-trespassory surveillances more common.\textsuperscript{80} Sotomayor noted that "in cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the \textit{Katz} analysis will require particular attention."\textsuperscript{81} In her

\begin{itemize}
\item \textsuperscript{71} \textit{Id.}
\item \textsuperscript{72} \textit{Id. at} 562.
\item \textsuperscript{73} \textit{Id. at} 563.
\item \textsuperscript{74} \textit{Id. at} 562.
\item \textsuperscript{75} United States v. Jones, 132 S. Ct. 945, 952 (2012).
\item \textsuperscript{76} \textit{Id. at} 951.
\item \textsuperscript{77} \textit{Id.} Specifically, the Court stated that "Fourth Amendment jurisprudence . . . [is] tied to common-law trespass." \textit{Id. at} 947.
\item \textsuperscript{78} \textit{Id. at} 951.
\item \textsuperscript{79} See generally \textit{id. at} 954.
\item \textsuperscript{80} \textit{Id. at} 955 (Sotomayor, J., concurring).
\item \textsuperscript{81} \textit{Id.}
\end{itemize}
view, GPS tracking provides a widespread and detailed record of an individual’s movements, thus reflecting details about “political, professional, religious, and sexual associations.” 82

Sotomayor argued that for future analyses courts should focus on whether an individual reasonably expects his or her movements to be recorded and gathered in a way that allows the government to discover personal details from the aggregate of the GPS tracking. 83 Most notably, Sotomayor concluded her concurrence by indicating the need to reconsider the third-party doctrine, as it is particularly unworkable in the current digital era, where large quantities of individual information are shared even in the most uninteresting transactions. 84 Although not adopted by the Supreme Court, the mosaic theory has gained some traction in certain courts, while others have deferred on the issue. 85

Two Supreme Court decisions predating Jones and focusing on a more rudimentary form of location tracking, the beeper, 86 frequently enter the CSLI discussion. 87 In United States v. Knotts, law enforcement officers installed a beeper inside a container the defendant was transporting. 88 Law enforcement then used the information generated from the beeper to create probable cause for a search warrant. 89 The Court held that the defendant had no reasonable expectation of privacy in his movement on public roads as it was tracked by the beeper. 90 In United States v. Karo, law enforcement officers obtained a court order to install a beeper on a can of ether the defendant would be carrying. 91 There, the Court found

82. Id.
83. Id. at 956.
84. Id. at 957.
85. Compare United States v. White, 62 F. Supp. 3d 614, 623 (E.D. Mich. 2014) (citing to Justice Sotomayor’s concurring opinion in Jones to find there was a violation of a reasonable expectation of privacy in the month-long tracking of a defendant’s cell phone location), with United States v. Ashburn, 76 F. Supp. 3d 401, 414 (E.D.N.Y. 2014) (declining to decide admissibility of long-term location tracking information under the mosaic theory, but utilizing a good faith exception instead).
86. Beepers are “battery-powered radio transmitter[s] that emit recurrent signals at a set frequency.” Note, Tracking Katz: Beepers, Privacy and the Fourth Amendment, 86 YALE L.J. 1461, 1461 (1977). When the beepers are attached to an object, the location of the beeper and object can be monitored for extended periods of time via a receiver to which the beeper transmits signals. Id.
88. Knotts, 460 U.S. at 278.
89. Id. at 279.
90. Id. at 285.
91. Karo, 468 U.S. at 708.
the government’s monitoring or location tracking of the beeper constituted a search because it tracked the defendant while he was in his home.\(^{92}\)

Both *Knotts* and *Karo* clarify where there is a reasonable expectation of privacy in terms of location tracking. More importantly, however, they also necessarily implicate the distinction between GPS tracking implemented by the government and location information collected by a third party and later obtained by the government.\(^{93}\) As such, they are often cited to or distinguished in cases involving CSLI as an important part of Supreme Court precedent shaping these decisions.\(^{94}\) Both of the beeper cases demonstrate the Court’s willingness to protect an individual’s reasonable expectation of privacy in her location, so long as the government is the entity carrying out the activity.\(^{95}\)

Recently, the Supreme Court again showed a willingness to protect individual privacy in the face of government intrusion.\(^{96}\) In *Riley v. California*, the Court expanded Fourth Amendment protection to cell phones in specific circumstances.\(^{97}\) While the Court in *Riley* was concerned only with searches of cell phone contents in searches incident to arrest, much of the Court’s reasoning extended some of the principles of the mosaic theory to cell phone technology.\(^{98}\) Specifically, the Court noted that the information contained in a cell phone reveals significant personal details when viewed comprehensively, and that “the sum of an individual’s private life can be reconstructed” through the various pictures, locations, and information stored on the phone.\(^{99}\) Interestingly, the Court referenced *Jones* and acknowledged that “[h]istoric location information is a standard feature of many smart phones and can reconstruct someone’s specific movements down to the minute.”\(^{100}\)

---

92. *Id.* at 714.

93. See In re Application of the U.S. for Historical Cell Site Data (In re Application Fifth Circuit), 724 F.3d 600, 609 (5th Cir. 2013). The Fifth Circuit distinguished *Karo* from *Smith* on the basis that in *Karo*, “the Government was the one collecting and recording the information.” *Id.* The court also stated that for Fourth Amendment intrusions, the finding of a search is dependent on whether the government or a third party collects the information. *Id.* at 610.

94. See, e.g., Graham I, 796 F.3d 332, 347 (4th Cir. 2015) (distinguishing CSLI from the beepers in *Karo*, as CSLI can reveal more information); United States v. Wheeler, 169 F. Supp. 3d 896, 903 (E.D. Wis. 2016) (summarizing the *Karo* holding as important Supreme Court precedent when deciding on a CSLI Fourth Amendment search).

95. In re Application Fifth Circuit, 724 F.3d at 610.


97. *Id.* at 2485.

98. See generally *id.* at 2489.

99. *Id.*

100. *Id.* at 2490.
Ultimately, the Court held that police were required to obtain a warrant before searching cell phones seized on suspects; specifically noting that the personal information accumulated from technology does not lose its right to Fourth Amendment protection simply because individuals carry such information with them.\textsuperscript{101} This varied precedent indicates a trend by the Supreme Court towards recognizing that technology challenges traditional Fourth Amendment application and that there is a need to adequately protect location information under these changing circumstances. Despite this trend, the precedent above does not apply specifically to CSLI, so the third-party doctrine still controls CSLI cases decided by lower courts.

\section*{IV. Circuit Split and Realignment}

Since the Supreme Court has failed to address where CSLI falls within the evolving precedent of the third-party doctrine and the mosaic theory, circuit courts of appeals have been without guidance when facing this issue. During 2015 alone, three federal circuits ruled differently on the Fourth Amendment protection of CSLI with varying rationales.\textsuperscript{102} The circuit split seemed to resolve in 2016 with the circuits agreeing again, at least for now.\textsuperscript{103} However, the previous circuit split and recent realignment provide insight into how courts are grappling with CSLI and show that they are still in need of resolution from a higher authority.\textsuperscript{104}

\textsuperscript{101.} Id. at 2495.
\textsuperscript{102.} Compare United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) (holding the collection of CSLI was not a search under the Fourth Amendment, focusing on CSLI as non-content used for business purposes), and United States v. Davis, 785 F.3d 498, 507 (11th Cir. 2015) (applying the third-party doctrine and holding that the government’s acquisition of CSLI was not a Fourth Amendment search), with Graham I, 796 F.3d 332, 361 (4th Cir. 2015) (declining to apply the third-party doctrine and holding that there is a reasonable expectation of privacy in CSLI).
\textsuperscript{103.} \textit{Does Seeking Cell Site Location Information Require a Search Warrant?}, COLUMBIA LAW CAPT (Aug. 2009), http://web.law.columbia.edu/sites/default/files/microsites/public-integrity/files/does _seeking_cell_site_location_information_require_a_search_warrant_-_wesley_cheng-_august2016update_-_0.pdf. Following Graham II, the circuit courts of appeals may now be in agreement that CSLI does not warrant Fourth Amendment protection. Id. However, most other circuits have still not ruled on this issue, and while district courts have mostly conformed, some have not. Id.
\textsuperscript{104.} Robinson Meyer, \textit{No One Will Save You from Cellphone Tracking}, THE ATLANTIC (June 2, 2016), http://www.theatlantic.com/technology/archive/2016/06/fourth-circuit-csli-cellphone-location-tracking-legal/485225/. As noted by Orin Kerr, it will likely not be long before the Supreme Court rules on the CSLI issue, as all it would take is at least one jurisdiction to go against the grain by providing Fourth Amendment protection. Id.
A. Eleventh Circuit Approach

The Eleventh Circuit Court of Appeals, facing an issue of first impression, was asked to determine the place of CSLI in the scope of the Fourth Amendment in *United States v. Davis*. In *Davis*, the defendant was convicted for various armed robberies with evidence including his CSLI, which the government obtained by compelling its production from the cell phone carrier’s business records. The defendant argued that the compelled production of these records constituted a Fourth Amendment search requiring probable cause. The court held that the SCA order used to compel production of the CSLI was not a search under the Fourth Amendment, because there was no reasonable expectation of privacy in a third party’s business records. The court found that since the records were non-content under the SCA, the defendant had neither a property interest in the records, nor a subjective or objective reasonable expectation of privacy in them.

The Eleventh Circuit rejected the defendant’s argument to apply *Jones*, which held that attaching a GPS tracking device was a physical intrusion requiring a search warrant. The Eleventh Circuit distinguished CSLI from real-time GPS tracking, finding CSLI to be less precise in pinpointing location than GPS data. Analyzing the concurring opinions in *Jones*, the Eleventh Circuit declined to apply the mosaic theory approach as well. The court found that the concurring opinions “underscore[d] why this [c]ourt is bound by [the third-party doctrine].” Reading Justice Sotomayor’s concurrence, the court found the questions it raised to be simply that: questions. While acknowledging that Justice Sotomayor may have hinted at the need to reevaluate the third-party doctrine in the modern context, the court emphasized that she still ultimately concurred in the physical trespass holding of the majority. As a result, her subsequent questions or statements were not binding.

105. See generally 785 F.3d 498, 500 (11th Cir. 2015).
106. Id. at 501.
107. Id. at 503.
108. Id. at 507 (citing Smith v. Maryland, 442 U.S. 735 (1979)).
109. See supra notes 29-31 and accompanying text.
110. United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015).
112. Davis, 785 F.3d at 514.
113. Id.
114. Id.
115. Id.
116. Id.
117. Id.
The Eleventh Circuit strictly applied the third-party doctrine, recognizing that even if obtaining CSLI constituted a search, it was not unreasonable because there is no reasonable expectation of privacy in business records created and kept by a third party. The court chose not to discard the third-party doctrine simply because the records can reveal user location, even claiming that the records at issue in Smith technically revealed location as well since the information was tied to a landline home phone.

Finally, the court came back to the SCA as the ultimate guide, emphasizing that the reasonable suspicion requirement prior to obtaining a court order for CSLI constitutes built-in statutory privacy protections. The court determined that because CSLI is crucial in investigations, the SCA was intended to build probable cause rather than require it. As a result, the Eleventh Circuit ultimately concluded there was no Fourth Amendment search when the government obtained a defendant’s CSLI under the SCA.

B. Sixth Circuit Approach

After the Eleventh Circuit decision in Davis, the Sixth Circuit confronted the same issue in United States v. Carpenter, where the defendant was convicted of robbery with CSLI evidence obtained under the SCA. Although reaching a similar result as the Eleventh Circuit in finding that acquiring CSLI was not a search under the Fourth Amendment, the Sixth Circuit deviated slightly in its reasoning. The court focused upon the general non-content nature of CSLI in relation to traditional Fourth Amendment law, even without the SCA distinction as such. Specifically, the court likened CSLI to address information found on the outside of mail envelopes, as opposed to the letters inside the envelopes. Authority has long held that the information written on the outside of mail envelopes is non-content, as it only relays routing details for business purposes. Following this rationale, the court decided that

118. Id. at 517.
119. Id. at 511-12.
120. Id. at 517.
121. Id. at 518. Specifically, the court notes that SCA orders like the one here help to build probable cause, “[d]eflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources.” Id.
122. Id. at 511.
123. United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).
124. Id. at 890.
125. Id. at 887.
126. Id. at 886.
127. Id.
CSLI is used only for routine business purposes and thus does not share the same level of protection afforded to the content of the communications.128

Similar to the Eleventh Circuit, the Sixth Circuit rejected the defendant’s argument to expand the Jones holding to CSLI.129 The Sixth Circuit distinguished CSLI from the GPS tracking in Jones on two points.130 First, the GPS intrusion in Jones was a physical trespass, whereas the search here was into third party business records.131 Second, the GPS tracking in Jones had the potential to reveal detailed information, which CSLI could not do.132 The court would not extend the concept of the mosaic theory to CSLI, claiming that CSLI could not provide location information with the precision that other forms of GPS tracking could.133

The Sixth Circuit relied primarily upon the third-party doctrine and found it to be appropriate to address the issue of CSLI as well as to distinguish Jones, which was a physical trespass by the government, not a compelled production of third party records.134 The court emphasized the distinction between the government actions in both cases.135 The CSLI obtained in Carpenter was from a third-party’s business records, so the defendant had a diminished expectation of privacy with regards to those records.136 In contrast, the information obtained in Jones was not first revealed to a third party, but rather directly tracked by the government.137 As a result, the expectation of privacy and the type of government intrusion in the present case were fundamentally different from those in Jones.138

The Sixth Circuit rationalized that collecting CSLI contained in business records was squarely within the third-party doctrine, in stark contrast to the warrantless attachment of a GPS device to an

128. Id. at 887.
129. Id. at 888.
130. Id.
131. Id. at 889.
132. Id. (citing United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring)).
133. Id.
134. Id. Using traditional trespass principles, the Court in Jones held that law enforcement is required to obtain a warrant prior to attaching a GPS tracking device to a defendant’s vehicle for long-term location tracking. United States v. Jones, 132 S. Ct. 945, 949 (2012).
135. Carpenter, 819 F.3d at 888.
136. Id. at 889.
137. Id. at 888. Specifically, the court compared and contrasted the differences between the type of government action. Id. For example, the court noted that while the government’s wiretap of a telephone conversation would invade a reasonable expectation of privacy, that same conversation overheard on an airplane would not. Id.
138. Id. at 889.
individual's car as in Jones. Ultimately, the Sixth Circuit concluded that procuring CSLI was not a search, CSLI is appropriately protected by the SCA, and any reevaluation of how CSLI is obtained by law enforcement should be done by the legislature.

C. Fourth Circuit Approach

Under facts similar to Carpenter, the Fourth Circuit Court of Appeals was the first circuit court to define the Fourth Amendment protection given to CSLI in a vastly different way in its decision in Graham I. Although the Fourth Circuit did grant a rehearing en banc and eventually aligned its position with the Eleventh and Sixth Circuits, the rationale behind Graham I provides valuable insight on the divide regarding how to treat CSLI. In Graham, law enforcement officers sought disclosure of CSLI under the SCA for calls and text messages from two defendants convicted of robbery.

The Fourth Circuit initially held that when law enforcement officers obtain historic CSLI, they conduct a search within the meaning of the Fourth Amendment. The court in Graham I found that CSLI searches track movements and reveal personal details in which cell phone users have a reasonable expectation of privacy. The court cited to the beeper cases, Karo and Knotts, to establish the premise that “the Supreme Court has recognized an individual’s privacy interests in comprehensive accounts of her movements in her location . . . particularly when such information is available only through technological means not in use by the general public.” The court was particularly concerned about the long-term tracking device, the cell phone, being carried on the person, because it could track the individual even while at the home, a place where Fourth Amendment protection is at its strongest. As a result, the court in Graham I declined the rationale of the other circuits, finding

139. Id.
140. Id. at 890.
141. Graham I, 796 F.3d 332, 338 (4th Cir. 2015).
142. See generally Graham II, 824 F.3d 421 (4th Cir. 2016).
143. Graham I, 796 F.3d at 341.
144. Id. at 344-45.
145. Id. at 345.
146. In Karo, the Court found that a warrant was required when a location tracking beeper tracked a defendant in his house. United States v. Karo, 468 U.S. 705, 714 (1984). On the other hand, in Knotts, the Court found that there was no Fourth Amendment search when a beeper tracked the defendant on public roads. United States v. Knotts, 460 U.S. 276, 285 (1983).
147. Graham I, 796 F.3d at 345.
148. Id. at 347; see also Karo, 468 U.S. at 714 (noting the established principle that “private residences are places in which the individual normally expects privacy free of government intrusion”).
CSLI was fundamentally similar to other types of location tracking, despite the presence of a third party.\(^{149}\)

The court in *Graham I* addressed both the *Jones* holding as well as the third-party doctrine while affording CSLI the greatest protection under the Fourth Amendment seen thus far by a court.\(^{150}\) While analyzing the majority and concurring opinions in *Jones*, the Fourth Circuit found that the privacy interests implicated in *Jones* were equal to, if not greater than, the privacy interests in CSLI.\(^{151}\) Further, since the long-term location information comprehensively reveals details of an individual’s life, a search into CSLI invades a reasonable expectation of privacy.\(^{152}\)

While addressing the third-party doctrine, the *Graham I* court focused primarily on voluntary conveyance of information as the determining factor for assumption of risk.\(^{153}\) The court declined to extend the third-party doctrine to cell phones, as “a cell phone user does not ‘convey’ CSLI to her service provider at all,” and thus does not assume the risk that such information will be disclosed.\(^{154}\) Additionally, the court did not extend the third-party doctrine, because it found that the doctrine should not be categorically applied when there is a reasonable expectation of privacy in information “generated and recorded by a third party through an accident of technology.”\(^{155}\) The *Graham I* court concluded that individuals have a reasonable expectation of privacy in CSLI, implicating Fourth Amendment protection.\(^{156}\) As a result, law enforcement officers in the Fourth Circuit would have to obtain a warrant based on probable cause before collecting CSLI in the future.\(^{157}\)

After a rehearing en banc, the Fourth Circuit joined the Eleventh and Sixth Circuits, acknowledging that “[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine,” or “Congress may act to require a warrant for CSLI.”\(^{158}\) However, until that time, the Fourth Circuit determined it was bound by existing precedent, which required a finding that warrantless acquisition of CSLI did not violate the Fourth Amendment.\(^{159}\) The court

---

\(^{149}\) *Graham I*, 796 F.3d at 361.

\(^{150}\) Id.

\(^{151}\) Id. at 348.

\(^{152}\) Id.

\(^{153}\) Id. at 354.

\(^{154}\) Id.

\(^{155}\) Id. at 360.

\(^{156}\) Id. at 361.

\(^{157}\) Id.

\(^{158}\) *Graham II*, 824 F.3d 421, 425 (4th Cir. 2016).

\(^{159}\) Id.
in *Graham II* found that the defendant mischaracterized the governmental activity by relying upon the beeper cases.\(^{160}\) The court rejected the notion that the beeper cases stood for the proposition that there is an individual expectation of privacy when location is being tracked.\(^{161}\) Rather, the court drew upon the third-party doctrine and distinguished how this case involved government collection of third party records, not government tracking of individuals.\(^{162}\) Like the Sixth Circuit, the Fourth Circuit in *Graham II* found the nature of the government activity to be different in cases of CSLI, because law enforcement was not actively tracking a defendant, but rather obtaining third-party records.\(^{163}\)

From there, the court in *Graham II* applied the third-party doctrine as set forth in *Smith*, finding CSLI to be analogous to the telephone numbers recorded by a pen register.\(^{164}\) According to the court, CSLI was voluntarily conveyed and “unquestionably ‘exposed,’” thus the defendants assumed the risk that the information would be disclosed to the government.\(^{165}\) As a result, the court held that government acquisition of CSLI did not require a warrant based on probable cause as per the Fourth Amendment.\(^{166}\) The Fourth Circuit acknowledged that to hold otherwise, as the court did in *Graham I*, would be to conflict with binding Supreme Court precedent and the majority of other federal circuits.\(^{167}\)

V. ARGUMENT

Neither the third-party doctrine nor the mosaic theory is an appropriate solution to protect CSLI under the Fourth Amendment. The Supreme Court should continue its trend of recognizing the unique role of new technology with regards to the Fourth Amendment and overturn the third-party doctrine as applied in such circumstances. However, the Supreme Court alone cannot be the only authority to define the place of CSLI in the Fourth Amendment scheme. Therefore, the legislature should take up the issue of CSLI

\(^{160}\) Id. at 426.
\(^{161}\) Id.
\(^{162}\) Id.
\(^{163}\) Id.; see also *In re Application Fifth Circuit*, 724 F.3d at 610 (emphasizing the importance of determining “who is recording an individual’s information initially,” as that determines the individual’s reasonable expectation of privacy) (emphasis in original).
\(^{164}\) *Graham II*, 824 F.3d at 427. Specifically, the court noted that the CSLI that the carrier recorded “was necessary to route Defendants’ cell phone calls and texts, just as the dialed numbers recorded by the pen register in *Smith* were necessary to route the defendant’s landline calls.” Id.
\(^{165}\) Id.
\(^{166}\) Id.
\(^{167}\) Id. at 429.
and enact a statute that protects this important information under the Fourth Amendment by requiring a warrant based on probable cause before it is collected.

A. Insufficiency of the Third-Party Doctrine and Mosaic Theory

The third-party doctrine is grounded in reasonable principles for the era in which it was created, but it does not translate into an age of technology.\textsuperscript{168} As such, the doctrine is insufficient to protect CSLI.\textsuperscript{169} The third-party doctrine is premised on the idea that information is voluntarily conveyed and courts allowing warrantless searches of CSLI have justified holdings based on this concept.\textsuperscript{170} However, by its very essence, cell phone technology challenges that foundational aspect of the third-party doctrine.\textsuperscript{171} CSLI is not voluntarily conveyed, but rather is automatically collected by service providers and not revealed to users.\textsuperscript{172} The user does not consent to or participate in the collection or transmission of the location at all besides simply using a personal piece of technology.\textsuperscript{173} In fact,

\begin{itemize}
\item \textsuperscript{168} United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Sotomayor stated that the third-party doctrine premise is “ill suited to the digital age,” and provided various examples of information disclosed to third parties, including URLs, emails, and phone numbers, which users would not wish to be disclosed without a warrant. \textit{Id.} As a result, Sotomayor concluded that she “would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” \textit{Id.}
\item \textsuperscript{169} See \textit{In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.}, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011). Specifically, the court for the Eastern District of New York stated:

\begin{quote}
The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by “choosing” to carry a cell phone must be rejected. In light of drastic developments in technology, the Fourth Amendment doctrine must evolve to preserve cell-phone user’s \textit{[sic.]} reasonable expectation of privacy in cumulative cell-site-location records.
\end{quote}
\textit{Id.}
\item \textsuperscript{170} \textit{Compare} United States v. Wheeler, 169 F. Supp. 3d 896, 910 (E.D. Wis. 2016) (rejecting the \textit{Graham I} court’s conclusion that a cell phone user does not voluntarily convey CSLI under the third-party doctrine), \textit{with} United States v. Rogers, 71 F. Supp. 3d 745, 750 (N.D. Ill. 2014) (finding no reasonable expectation of privacy in CSLI voluntarily conveyed to the cell phone carrier).
\item \textit{Graham I}, 796 F.3d 332, 354 (4th Cir. 2015). Specifically, the court in \textit{Graham I} noted that a “cell phone user does not ‘convey’ CSLI to her service provider at all—voluntarily or otherwise.” \textit{Id.}; see also \textit{In re Application Fifth Circuit}, 724 F.3d 600, 612 (5th Cir. 2013) (summarizing the American Civil Liberties Union argument that a cell phone user receives no indication that he will be located when making a call, thus “[a] user cannot convey something which he does not know he has”).
\item \textit{Graham I}, 796 F.3d at 354; see also Com. v. Augustine, 4 N.E.3d 846, 862 (Mass. 2014) (distinguishing CSLI from the phone numbers in Smith, because “no cellular telephone user . . . voluntarily conveys CSLI to his or her cellular service provider.”).
\item \textit{Graham I}, 796 F.3d at 354-55.
\end{itemize}
“CSLI is purely a function and product of cellular telephone technology, created by the provider’s system network.” As a result, CSLI is a natural consequence of cell phone technology, and law enforcement officers seek it not for any information voluntarily given by the user, but rather for the information’s “by-product” – the CSLI. Even conceding that the cell phone provider owns this information, CSLI is vastly different from the types of information the third-party doctrine originally anticipated. Given this, it cannot be said that cell phone users assume the risk of CSLI disclosure when they have not “actively” chosen to disclose it.

The basic third-party doctrine premise of voluntary conveyance is not the only issue preventing the doctrine from transitioning into the technological era. As noted by Justice Marshall in his Smith dissent, lack of alternatives makes the third-party doctrine particularly difficult to justify. In Smith, Marshall was concerned with the lack of alternative to the traditional landline home phone. Cell phones are arguably even more ubiquitous than home phones, thus escalating the concern originally presented by Justice Marshall. In fact, cell phones have been acknowledged to be “so pervasive that some persons may consider them to be essential means or necessary instruments of self-expression.” The lack of meaningful alternatives to a cell phone in the modern age makes it difficult to claim users could avoid unwanted effects of the third-party doctrine, like CSLI disclosure, simply by not owning a cell phone.  

174. Augustine, 4 N.E.3d at 862.
175. Id. at 863.
176. Id.
177. Graham I, 796 F.3d at 355.
179. Id.
180. Graham I, 796 F.3d at 355. In declining to accept the voluntary conveyance justification, the Graham I court stated:

We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the device on their person. Cell phone use is not only ubiquitous in our society today, but at least for an increasing portion of our society, it has become essential to full cultural and economic participation.

182. See Richard Brust, Crashing the Third Party: Experts Weigh How Far the Government Can go in Reading Your Email, A.B.A. (Aug. 1, 2012), http://www.abajournal.com/magazine/article/crashing_the_third_party_experts_weigh_how_far_the_government_can_go (discussing how there is “no practical alternative to use of [a] third party” when conveying information technologically, meaning the alternative is not to communicate at all); see also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) (acknowledging that cell phones have replaced...
Additionally, the argument that CSLI falls outside of Fourth Amendment principles simply because the government does not actively collect the information is without merit.\textsuperscript{183} \textit{Knotts} and \textit{Karo} implicate the same privacy interests as CSLI, despite their specific context of law enforcement officers actively tracking rather than obtaining third party records.\textsuperscript{184} Simply because CSLI is technically collected first by a third-party rather than the government should not preclude the information from the Fourth Amendment warrant requirement.\textsuperscript{185} The mechanism or party doing the collecting does not make the information revealed any less personal or any less worthy of protection.\textsuperscript{186}

Courts that have looked to the beeper cases, \textit{Knotts} and \textit{Karo}, when analyzing CSLI have done so not only for the third party versus government distinction, but also for the proposition that CSLI can track individuals in constitutionally protected places.\textsuperscript{187} By this logic, CSLI should fall within the Fourth Amendment’s protection, because cumulative and extended location tracking “implicates a privacy interest on the part of the individual who is the target.”\textsuperscript{188} While GPS trackers such as the one used in \textit{Jones}, or beepers in \textit{Knotts} and \textit{Karo}, are obviously distinct from CSLI in functionality, they both center around the same interest: an individual’s reasonable expectation of privacy in his movements.\textsuperscript{189} Since CSLI protects the same privacy interests that are at stake with GPS trackers, this information should not be precluded from Fourth Amendment protection solely because the government goes through an intermediary to obtain it.\textsuperscript{190}

\textsuperscript{183} See supra note 93 and accompanying text.
\textsuperscript{184} See Graham I, 796 F.3d at 346 (likening the search in \textit{Karo} to CSLI, as both searches “allow the government to place an individual and her personal property . . . at the person’s home and other private locations”).
\textsuperscript{186} See Graham I, 796 F.3d at 360 (remarking that the generation of CSLI is an incident of the technology, and the third-party doctrine is not intended “to diminish Fourth Amendment protections where new technology provides new means for acquiring private information”).
\textsuperscript{188} Id. citing United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).
\textsuperscript{189} Id. at 865. But see United States v. Davis, 785 F.3d 498, 515 (6th Cir. 2015) (distinguishing between real-time GPS tracking and CSLI by claiming CSLI is not as precise as GPS tracking nor does it warrant the same reasonable expectation of privacy).
\textsuperscript{190} \textit{In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.}, 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011).
The mosaic theory comes closer to accommodating the Fourth Amendment needs of evolving technology, but is still an insufficient solution to protect CSLI. The general concept of the mosaic theory, which encourages analyzing the government activity on the whole, moves Fourth Amendment jurisprudence into the twenty-first century by acknowledging that metadata poses challenges to existing rules of law. However, implementation of the mosaic theory would require courts to define an entirely new doctrine of Fourth Amendment law, an arduous task involving novel questions.

The primary concern with the mosaic theory is that it is stand-alone, which is a problem not easily cured. As a result, the mosaic theory is not a viable option for the Supreme Court to turn to in the upcoming Carpenter case. Courts implementing the theory would be required to determine at what stages of surveillance it applies. For example, whether the mosaic theory applies only to collection of data, analysis of the data following collection, or both. Along the same lines, courts would be forced to define clearer standards with regards to which surveillance methods the theory applies. This task would also involve determining whether different methods should be grouped together as part of one mosaic. For example, if law enforcement used GPS tracking, CSLI, and a surveillance camera to track an individual, courts would need to determine if all of those methods should be grouped together or looked at separately in deciding if there is a Fourth Amendment search under the mosaic theory. Additionally, the mosaic theory complicates the concept of reasonableness that has become so foundational to the understanding of the Fourth Amendment. Courts using the mosaic theory would need to determine when such searches are reasonable, as well as when they require

192. Kerr, supra note 18, at 329.
193. Id. at 330.
enter-v-united-states-the-fourth-amendment-historical-cell-site-case/?utm_term=.4259d11f&802.
195. Id. at 329.
196. Id.
197. Id.
198. Id.
199. Id. at 334. Other parts of this inquiry include whether the mosaic theory should apply only to location surveillance, and whether different officers and investigations should be considered as part of the mosaic grouping. Id.
200. Id. at 336.
warrants based on probable cause or simply reasonable suspicion.201

Last, courts would have to determine what remedies should exist for searches found to be unconstitutional under the mosaic theory.202 This question involves resolving who has standing, the application of the fruit of the poisonous tree doctrine, and whether the exclusionary rule should be categorically applied.203 Overall, the mosaic theory presents a better solution than the third-party doctrine, but it would be cumbersome for The Supreme Court to implement and may perhaps only lead to more questions than answers.204 Moreover, these issues underscore the importance that a solution to CSLI gathering be a product of both legislation and case law.

B. The Solution: A Blend of the Judiciary and the Legislature

While it would be desirable for the Supreme Court to address the CSLI issue in its entirety, the holding would be limited to the facts and circumstances of Carpenter, and could leave open various questions for future litigation. For example, the Carpenter holding could not cover all related cell phone location information that originates from other sources such as cell site stimulators or GPS receivers within the cell phone.205 Further, even in finally addressing CSLI while deciding Carpenter, the judiciary cannot serve the law-making function as efficiently and re-write the outdated aspects of the SCA. The most effective way to accomplish securing Fourth Amendment protection for CSLI and begin a trend of increasing privacy protection for all new technologies is only with action from both the Supreme Court and Congress.

1. Overruling the Third-Party Doctrine in Carpenter

Although the Supreme Court cannot alone cure the entire CSLI problem when deciding Carpenter, it should abandon use of the third-party doctrine in technology cases, as the doctrine is unworkable in the modern context. To allow the third-party doctrine to perpetuate and permeate the field of technological communications

201. Id.
202. Id. at 340.
203. Id.
204. Id. at 329.
would come at the expense of significant individual privacy rights. Rather, the Supreme Court should take Carpenter as an opportunity to reevaluate the third-party doctrine and limit its use in the modern era.

On the questionable basis of voluntary conveyance, the third-party doctrine relegates the vast quantity of information contained in CSLI to the same status as records of phone numbers dialed from a landline phone in the 1970s. This is a stretched comparison that lacks applicability to CSLI, as CSLI provides significantly more information than simply telephone numbers dialed. CSLI is routinely generated as a result of the cell phone’s core function, much like most technology today, and thus cannot be considered to be voluntarily conveyed by users as required by the third-party doctrine. As discussed by the dissenting judges in Graham II, third-party doctrine precedent appears to demonstrate that voluntary conveyance requires both an individual’s knowledge and action. However, it is quite likely that the majority of cell phone users are unaware that they are conveying their location on a regular basis, which greatly undercuts the knowledge aspect of voluntary conveyance. Even if users possess a vague understanding of the technology involved when a cell phone connects to the network, they do not know through which tower the call is connecting, which again weakens the knowledge component of the conveyance.

Additionally, users do not actively transmit CSLI, but rather the information is automatically generated as part of the cell phone’s technology. Since cell phone users do not actively transmit CSLI nor possess the requisite knowledge of its transmission, CSLI is not voluntarily conveyed. This crucial fact demonstrates not only


207. Graham II, 824 F.3d 421, 436 (4th Cir. 2016) (noting that intrinsic to the third-party doctrine “is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy”).

208. Commonwealth v. Augustine, 4 N.E.4d 846, 863 (Mass. 2014). The Massachusetts Supreme Court noted that CSLI may reveal a “treasure trove of very detailed and extensive information about the individual’s ‘comings and goings’ in both public and private cases.”

209. Id. at 862.

210. See supra note 171 and accompanying text.

211. Graham II, 824 F.3d at 443 (Wynn, J., dissenting). The knowledge requirement involves the individual being aware she is “communicating particular information.” Id. The action requirement involves the defendant actively transmitting the information, such as through dialing or speaking. Id.

212. Id. at 445 (citing In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’ns Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 317 (3d Cir. 2010)).

213. Id.

214. Id.

215. Id. at 446.
that CSLI cannot be reconciled with the third-party doctrine, but also that new technologies on the whole are a poor fit with the doctrine. For example, the third-party doctrine has been invoked by various circuit courts of appeals to diminish Fourth Amendment protection for IP addresses, email addresses, and other information that must be transmitted to a third party out of necessity for the technology to operate.\footnote{See, e.g., United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016) (holding that under the third-party doctrine, an email user had no reasonable expectation of privacy in his IP address); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (relying on the third-party doctrine to establish that internet users have no reasonable expectation of privacy in email addresses).}

The third-party doctrine also lacks applicability to CSLI because the reasonable expectation of privacy in cell phone and location information is different than that for typical business records.\footnote{See United States v. Davis, 785 F.3d 498, 507 (11th Cir. 2015) (applying the third-party doctrine to hold there is no reasonable expectation of privacy in CSLI).} Although courts declining to extend Fourth Amendment protection to CSLI argue that there is no reasonable expectation of privacy in third party records,\footnote{See United States v. Davis, 785 F.3d 498, 507 (11th Cir. 2015) (applying the third-party doctrine to hold there is no reasonable expectation of privacy in CSLI).} CSLI implicates more than simple business records.\footnote{Earls, 70 A.3d at 642.} Rather, when CSLI is obtained, cell phones essentially function as tracking devices, providing significant amounts of personal information about an individual’s movements.\footnote{See Susan Freiwald, The Vanishing Distinction Between Real-time and Historical Location Data, CONCURRING OPINIONS (July 17, 2012), https://concurringopinions.com/archives/2012/07/the-vanishing-distinction-between-real-time-and-historical-location-data.html.} This occurs regardless of if the CSLI is historical or real time, as the information remains the same in either context.\footnote{Earls, 70 A.3d at 642. Specifically, the defendant in Earls was in a motel room while he was being tracked. Id. As a result, law enforcement officers were able to track the defendant in private spaces without a warrant, as they did not know in advance where the defendant would be going. Id.} The movements tracked include those in public as well as both constitutionally protected spaces and spaces where an individual maintains a reasonable expectation of privacy.\footnote{See Brief for Electronic Frontier Foundation, et al., as Amici Curiae Supporting Petitioner, United States v. Carpenter, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16-402).} In fact, organizations in favor of protecting CSLI argue that the compilation of location data implicates both First and Fourth Amendment protections, as the picture painted by location data can reveal political associations, religious affiliations, and other “expressive and associational activities.”\footnote{See Brief for Electronic Frontier Foundation, et al., as Amici Curiae Supporting Petitioner, United States v. Carpenter, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16-402).}
This pervasive nature of cell phones and the vast quantity of information contained in CSLI undercuts not only the voluntary conveyance argument, but also stands for the proposition that reasonable expectations of privacy have changed in the technological era.\textsuperscript{224} Because third parties are a necessary aspect of modern communication, it is no longer feasible to claim that the vast quantity of both content and non-content information transmitted to those third parties is not reasonably expected to be private.\textsuperscript{225} By reconsidering the third-party doctrine, the Supreme Court must also redefine the \textit{Katz} analysis to accommodate the constant presence of third parties in modern technology.

The inapplicability of third-party doctrine principles aside, the Supreme Court itself has not invoked the doctrine in recent years when presented with the opportunity to do so. This could be seen in \textit{Jones} for example, where the Court mentioned \textit{Smith} in passing, but did not engage in a discussion regarding its application to location decisions, resorting instead to traditional property principles for resolution.\textsuperscript{226} Additionally, the Court did not cite or give any mention to the third-party doctrine in \textit{Riley}, even while discussing the fact that cell phone information may be stored on a third party cloud.\textsuperscript{227} The Supreme Court's lack of acknowledgment of its own doctrine in recent cases of location tracking and cell phone privacy further demonstrates that the third-party doctrine has lost applicability in the modern context and should be overturned as a precedent in such contexts.\textsuperscript{228}

One court even compiled the most recent Supreme Court precedent, including \textit{Riley}, \textit{Jones}, \textit{Knotts}, and \textit{Karo} to acknowledge that these decisions together create a new set of Fourth Amendment principles for cell phone tracking.\textsuperscript{229} Analyzing these decisions as a composite, the district court for the Northern District of California synthesized the following three principles:

(1) an individual’s expectation of privacy is at its pinnacle when government surveillance intrudes on the home; (2) long-term electronic surveillance by the government implicates an individual’s expectation of privacy; and (3) location data generated

\begin{itemize}
  \item \textsuperscript{224} United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
  \item \textsuperscript{225} \textit{Id.}; see also generally United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
  \item \textsuperscript{226} \textit{Jones}, 132 S. Ct. at 950.
  \item \textsuperscript{227} \textit{Riley} v. California, 134 S. Ct. 2473, 2491 (2014).
  \item \textsuperscript{228} \textit{Id.}
  \item \textsuperscript{229} \textit{In re Application for Tel. Info. Needed for a Criminal Investigation}, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015).
\end{itemize}
by cell phones, which are ubiquitous in this day and age, can reveal a wealth of private information about an individual.\textsuperscript{230}

Arguably, these three principles indicate how the Supreme Court has moved away from the third-party doctrine and at least implicitly acknowledged some reasonable expectation of privacy in cell phones.\textsuperscript{231} Further, although these principles were compiled with regards to active government tracking with a beeper, they are equally applicable to both historical and real-time CSLI.\textsuperscript{232}

This shift in precedent from the third-party doctrine can be explained by Professor Orin Kerr’s “equilibrium adjustment” theory.\textsuperscript{233} Under this theory, the Supreme Court’s Fourth Amendment precedent can be analyzed as part of a longstanding tradition of Fourth Amendment adjustments to obtain equilibrium between individual privacy and government interests.\textsuperscript{234} As per the equilibrium adjustment approach, the Court adopts broad Fourth Amendment principles when changing technology makes it difficult for law enforcement to obtain evidence.\textsuperscript{235} Conversely, when technological advancements make it easier for law enforcement to obtain evidence, the Court alters the Fourth Amendment principles “to try to restore the prior equilibrium,” in favor of privacy.\textsuperscript{236} It is argued that under this theory, the Court should wait until a technology has reached a point of stability before intervening to restore privacy protections.\textsuperscript{237}

This approach further explains the Court’s recent shift to protect individual privacy in technology and why the Court should use Carpenter as an opportunity to abandon the third-party doctrine,\textsuperscript{238} in order to restore individual privacy, as part of its natural return to more privacy protection.\textsuperscript{239} CSLI is not a new development and it continues to serve as the foundation for basic cell phone technology, even as phones are updated and changed to possess more location

\textsuperscript{230} Id.
\textsuperscript{231} Id.
\textsuperscript{232} Id. at 1031. Specifically, the court compared CSLI to the beepers used in Karo, as both can reveal information that would be otherwise unavailable to law enforcement without a warrant based on probable cause. Id.
\textsuperscript{234} Id.
\textsuperscript{235} Id. at 480.
\textsuperscript{236} Id.
\textsuperscript{237} Id. at 482.
\textsuperscript{238} See generally Riley v. California, 134 S. Ct. 2473 (2014).
In order for the Fourth Amendment to remain relevant and applicable in the modern context, its interpretation must be flexible and changing to accommodate evolving technology.\footnote{240} The Sixth Circuit’s heavy focus upon the third-party doctrine in its analysis in \textit{Carpenter} provides a perfect opportunity for the Supreme Court to reconsider the third-party doctrine.\footnote{241} Indeed, the Court’s grant of certiorari on a CSLI case at this time when the circuit courts of appeal are in agreement raises the inference as to whether the Court intends to do just that.\footnote{242} This is further supported by the fact that the Court did not grant certiorari to \textit{Davis} or \textit{Graham II}, both of which were also appealed.\footnote{243} Rather, the Court has decided to hear \textit{Carpenter} alone, denying certiorari to \textit{Davis} and choosing not to act on the \textit{Graham II} certiorari petition.\footnote{244}

Additionally, the current composition of the Supreme Court gives some indication that the third-party doctrine may be reconsidered and altered in the upcoming \textit{Carpenter} case. Justice Sotomayor has already voiced her concern regarding comprehensive location data and the third-party doctrine’s inapplicability in the “digital age.”\footnote{245} While no other justices joined Justice Sotomayor in \textit{Jones}, Justices Ginsburg, Breyer, and Kagan, joined Justice Alito’s separate concurrence, which at least indicated a concern regarding the ease of tracking location with the emergence of new technology.\footnote{246} Further, Chief Justice Roberts authored the landmark opinion \textit{Riley}, which recognized the need to protect the extensive personal data contained in personal cell phones.\footnote{247} Although newly appointed Justice Gorsuch’s opinions on the third-party doctrine are somewhat unknown, he did acknowledge the uncertainty surrounding the doc-

\footnote{240. \textit{See} Brief for the American Civil Liberties Union et al. as Amici Curiae Supporting Appellant, United States v. Carpenter, 819 F.3d 990 (6th Cir. 2016). In its brief, the American Civil Liberties Union also discusses the creation of newer, smaller cells, including microcells, picocells, and femtocells, which “provide service to areas as small as ten meters.” \textit{Id.} Thus, location in these newer cells can be tracked through CSLI even more precisely than before. \textit{Id.}}

\footnote{241. \textit{In re} Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011).}

\footnote{242. United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016).}

\footnote{243. \textit{See supra} note 158 and accompanying text.}

\footnote{244. \textit{See} \textit{Graham II}, 824 F.3d 421 (4th Cir. 2016), \textit{petition for cert. filed}, (U.S. Sept. 26, 2016) (No. 16-6308); United States v. Davis, 785 F.3d 498 (11th Cir. 2015), \textit{cert. denied}, 84 U.S.L.W. 3081 (U.S. Nov. 9, 2015) (No. 15-146).}


\footnote{247. \textit{Id.} at 963 (Alito, J., concurring).}

\footnote{248. Riley v. California, 134 S. Ct. 2473, 2495 (2014).}
trine in a Tenth Circuit decision where he found email communications are protected by the Fourth Amendment.\textsuperscript{249} The Supreme Court should continue its trend of increasing Fourth Amendment protection for new technologies by using \textit{Carpenter} to overrule the third-party doctrine’s application in CSLI and future cases implicating third-parties in technology.

2. \textit{Congressional Action: Requiring Probable Cause}

The Supreme Court is not and cannot be the only entity the public must rely on to protect CSLI\textsuperscript{250}. The SCA may have been appropriate legislation at the time it was passed, but Congress surely did not envision the sensitive information currently proliferated by new technology when it created a lower cause standard for non-content.\textsuperscript{251} The legislative branch is better suited to determine the public opinion on issues of this nature and balance governmental interests with privacy rights.\textsuperscript{252} Congress has at its disposal various resources that allow it to strike the balance better than courts may.\textsuperscript{253} Through access to expert opinions and testimony in legislative hearings, Congress can receive the information necessary to weigh the interests of investigation techniques with constitutionally protected privacy rights.\textsuperscript{254}

Additionally, when Congress speaks through a statutory enactment, it creates clearer and more uniform standards upon which courts can rely, thus eliminating the legal uncertainty that comes with circuit splits.\textsuperscript{255} Unlike the Supreme Court, Congress can create broad protections for both real-time and historical CSLI through

\begin{itemize}
  \item 249. United States v. Ackerman, 831 F.3d 1292, 1304-05 (10th Cir. 2016).
  \item 250. \textit{See, e.g.}, Jones, 132 S. Ct. at 964 (Alito, J., concurring) (finding “[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative”); \textit{Graham II}, 824 F.3d 421, 436 (4th Cir. 2016) (stating “application of the third-party doctrine does not render privacy an unavoidable casualty of technological progress – Congress remains free to require greater privacy protection if it believes that desirable”).
  \item 252. \textit{Jones}, 132 S. Ct. at 964 (Alito, J., concurring).
  \item 253. \textit{Graham II}, 824 F.3d at 439 (Wilkinson, J., concurring). \textit{See also} United States v. Davis, 785 F.3d 498, 520 (6th Cir. 2015) (Pryor, J., concurring) (declining to extend Fourth Amendment protection to CSLI because Congress “has the institutional competence to evaluate complex and evolving technologies.”).
  \item 254. \textit{Graham II}, 824 F.3d at 440 (Wilkinson, J., concurring).
  \item 255. \textit{Id.}.
\end{itemize}
a statute rather than being limited to the circumstances surrounding one case.\textsuperscript{256} Overall, Congress is in the best position to determine how CSLI and indeed, all information proliferated by new technology, can coexist with government searches.\textsuperscript{257}

Perhaps the strongest argument for Fourth Amendment protection of CSLI is simply that CSLI is fundamentally different from the old technologies the precedent intends to accommodate. Telephone numbers revealed via a pen register or records of phone numbers dialed on a landline phone do not reveal nearly the volume of personal detail as do CSLI records.\textsuperscript{258} Although CSLI does not disclose as precise of a location as a GPS may, CSLI can lead to logical inferences that reveal not just location information, but also personal information about a user on the whole.\textsuperscript{259}

Along with these basic concerns about locational information, CSLI challenges the content and non-content distinction of the SCA era in the age of metadata.\textsuperscript{260} In fact, while most courts discount CSLI as non-content, “there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the government would be equally intrusive and reveal information society values as private.”\textsuperscript{261} The sheer breadth of information that CSLI and similar bulk data collections can reveal about an individual challenge not only the third-party doctrine, but also the non-content justification created by the SCA.\textsuperscript{262} All of these concerns make it imperative for Congress to finally define more clear lines in this area and increase Fourth Amendment protection for CSLI.

Congress should be motivated to take up this issue, as there is significant research indicating many Americans are concerned about their lack of privacy, both with the government and with companies facilitating communications.\textsuperscript{263} In the aftermath of the Snowden revelations, digital privacy has become more prevalent

\begin{itemize}
\item \textsuperscript{256} See Susan Freiwald, supra note 221.
\item \textsuperscript{257} Id. As noted by Judge Wilkinson, Congress has the power to add “democratic legitimacy to a high stakes and highly controversial area,” in the context of emerging communication technologies. Id.
\item \textsuperscript{258} See Brief for the American Civil Liberties Union, et al. as Amici Curiae Supporting Appellant, United States v. Carpenter, 819 F.3d 990 (6th Cir. 2016).
\item \textsuperscript{259} In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’ns Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 311 (3d Cir. 2010).
\item \textsuperscript{260} In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011).
\item \textsuperscript{261} Id.
\item \textsuperscript{262} See id.
\end{itemize}
and more frequently discussed in society.\textsuperscript{264} This concern directly implicates CSLI, as studies show that the American public considers location data and general cell phone communications to be sensitive information deserving privacy protection.\textsuperscript{265} These concerns regarding privacy of information expand beyond simply a fear of government,\textsuperscript{266} as many adults feel they have lost control over the use of their personal information that is gathered by companies too.\textsuperscript{267} Additionally, in light of the new Trump era, there is increased fear that the balance between personal privacy and government interests will become even more disparate.\textsuperscript{268} The American public's belief that location information is highly sensitive combined with the drastic increase in cell phone towers and usage that creates highly precise location data makes this a ripe issue for legislation.\textsuperscript{269} This information indicates that Congress should act on behalf of its constituents to protect information that citizens reasonably believe to be private.

As technologies continue to evolve, metadata consistently accumulates,\textsuperscript{270} and political rhetoric implies individual privacy must be traded off for security,\textsuperscript{271} Congress must be called upon to draw a clear line that preserves Fourth Amendment protection for CSLI. In fact, a bill was introduced in Congress in 2015 proposing greater

\begin{itemize}
\item \textsuperscript{264} Id.
\item \textsuperscript{265} Id. In 2014, half of college educated adults reported believing their individual location information gathered from a cell phone over a long period of time to be "very sensitive" information." Id. An additional 32% of college educated adults considered the information to be "somewhat sensitive." Id.
\item \textsuperscript{266} Only 6% of adults surveyed by Pew Research Center were confident that government agencies could keep their information private. Americans Attitudes About Privacy, Security and Surveillance, PEW RESEARCH CENTER, http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf (last visited Sept. 19, 2017). Only 6% of adults surveyed by Pew Research Center were confident that government agencies could keep their information private. Id.
\item \textsuperscript{267} Public Perceptions of Privacy and Security in the Post-Snowden Era, supra note 263. Specifically, Pew Research Center found that 91% of adults surveyed were concerned about their loss of privacy to third party companies. Id.
\item \textsuperscript{269} See supra notes 253-257.
\item \textsuperscript{270} See Alexander Galicki, The End of Smith v. Maryland?: The NSA’s Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age, 52 AM. CRIM. L. REV. 375, 389 (2015) (acknowledging that advancements in technology have caused exposure of metadata to telephone companies, Internet service providers, and other third parties).
\end{itemize}
protection for location data.\footnote{272} The Geolocation Privacy and Surveillance ("GPS") Act would require law enforcement officers to obtain a warrant pursuant to federal or state rules of criminal procedure prior to obtaining geolocation information.\footnote{273} The bill defines geolocation information to include "any information that is not the content of a communication, concerning the location of a wireless communication device."\footnote{274} This proposed legislation contained enumerated exceptions to the warrant requirement in the cases of emergency situations,\footnote{275} and provided for civil remedies in the event location information was obtained in violation of the statute.\footnote{276}

The proposed GPS Act would be a vital first step in protecting CSLI and other location information that is currently not covered by the SCA.\footnote{277} Congress should acknowledge that the content and non-content distinction of the past is blurred when metadata can provide similar individual personal details.\footnote{278} As part of this, Congress should amend the Stored Communications Act to comply with the Fourth Amendment without regard for the content and non-content distinction. Under the revised act, Congress should require a warrant based on probable cause be issued before any real-time or historical CSLI is obtained.

VI. CONCLUSION

CSLI is a microcosm demonstrating one way in which the courts and the law have not kept pace with current technologies.\footnote{279} So long as technologies continue to evolve and CSLI proliferates, the third-party doctrine will become strained,\footnote{280} and the mosaic theory

\begin{itemize}
\item \footnote{273} Geolocation Privacy and Surveillance Act, H.R. 491, 114th Cong. § 2602 (2015).
\item \footnote{274} Id. § 2601.
\item \footnote{275} Id. § 2604. Some exceptions include "immediate danger of death or serious physical injury," and "conspiratorial activities threatening the national security interest." Id.
\item \footnote{276} Id. § 2605. Possible damages may include injunctive relief and punitive damages. Id. Additionally, the statute provides that location information obtained in violation of the statute must be excluded as evidence. Id.
\item \footnote{277} See Wyden, Chaffetz Stand Up for Privacy with GPS Act, https://www.wyden.senate.gov/news/press-releases/wyden-chaffetz-stand-up-for-privacy-with-gps-act (last visited Jan. 28, 2017) (stating that the proposed legislation would "settle the controversy" regarding location information and "provide specific and clear guidelines to ensure this valuable and effective technology is not abused").
\item \footnote{278} Supra notes 260-261.
\item \footnote{279} See generally Jennifer Valentino-Devries, How Technology is Testing the Fourth Amendment, WALL STREET JOURNAL (Sept. 21, 2011, 10:32 PM) http://blogs.wsj.com/digits/2011/09/21/how-technology-is-testing-the-fourth-amendment/.
\item \footnote{280} See supra notes 206-208.
\end{itemize}
is not in any position to take its place.281 Both the judiciary and legislature must come together to protect individual privacy and move Fourth Amendment jurisprudence into the modern era by requiring warrants based on probable cause prior to the acquisition of reasonably private information.

281. See supra note 192.