SIXTH CIRCUIT REVIEW

A Growing Consensus: A Comment on *United States v. Carpenter*, and the U.S. Supreme Court's Opportunity to Protect Privacy

AARON STEVENSON*

Commenting on *United States. v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).

TABLE OF CONTENTS

I. INTRODUCTION

Be aware—if you are a resident of Michigan, Ohio, Kentucky, or Tennessee, the police can now obtain a record of your physical location without a court-issued warrant.[1] For cell phone owners in these states—which is nearly

* J.D. Candidate 2017, The Ohio State University Moritz College of Law; B.A., The Ohio State University. The Author would like to thank Professor Ric Simmons and the *Ohio State Law Journal* for their advice and feedback on this Comment.

[1] *See* United States v. Carpenter, 819 F.3d 880, 886–90 (6th Cir. 2016).

everyone[2]—the Sixth Circuit has determined that the Fourth Amendment does not protect your geographic cell site location information (CSLI).[3]

The Sixth Circuit joined a host of other circuits and dealt a blow to privacy rights when it decided *United States v. Carpenter*.[4] In *Carpenter*, the court found that an individual has no reasonable expectation of privacy in their CSLI.[5] CSLI is the geographic data that cell phone users generate and send to carriers during daily use of their cellular devices.[6] Wireless carriers store CSLI, and law enforcement can request the information.[7] This decision affects the privacy of millions of Americans who use their cell phones every day.

The decision comes at a time when courts are struggling to keep the Fourth Amendment updated with changing technology.[8] The Supreme Court has not helped with this endeavor—it has sidestepped several opportunities to help redefine the contours of the Fourth Amendment for a twenty-first century world.[9] On September 26, 2016, Carpenter filed a petition for a writ of certiorari and presented the Supreme Court with yet another opportunity to modernize the Fourth Amendment.[10] Hopefully the Supreme Court will not shy away from this moment.

---

[2] A recent report from the Pew Research Center shows that 95% of Americans now own some type of cell phone. *See Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/PGC3-67EZ]. Remarkably, 77% of Americans own a smartphone. *Id.*

[3] *See Carpenter*, 819 F.3d at 886–90.

[4] The Sixth Circuit's decision reached the same conclusion as the Fifth and Eleventh Circuits. *See* United States v. Davis, 785 F.3d 498, 500 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015); United States v. Guerrero, 768 F.3d 351, 358–59 (5th Cir. 2014) (following their own precedent established in *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013)), *cert. denied*, 135 S. Ct. 1548 (2015). Further, after *Carpenter*, the Fourth Circuit, in an en banc decision, reached the same conclusion on Fourth Amendment treatment of CSLI. *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc).

[5] *Carpenter*, 819 F.3d at 888.

[6] Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [https://perma.cc/9C53-TSHC]; *see also Carpenter*, 819 F.3d at 885.

[7] *See Carpenter*, 819 F.3d at 885.

[8] *See* Ric Simmons, *The Missed Opportunities of* Riley v. California, 12 OHIO ST. J. CRIM. L. 253, 253 (2014).

[9] For example, *Riley v. California*, 134 S. Ct. 2473 (2014), *United States v. Jones*, 565 U.S. 400 (2012), and *City of Ontario v. Quon*, 560 U.S. 746 (2010), are all recent cases where the Supreme Court has either avoided a Fourth Amendment question or limited their holding to the specifics of the case before them. *See* Aaron Stevenson, *A Fourth Amendment Framework for the Future: Applying the Mosaic Theory to Digital Communications*, 77 OHIO ST. L.J. FURTHERMORE 145, 150 & n.32 (2016). For an argument that the Supreme Court has been too hesitant to update the Fourth Amendment with new technology, see generally Simmons, *supra* note 8.

[10] Petition for a Writ of Certiorari, Carpenter v. United States, No. 16-402 (Sept. 26, 2016); *Carpenter v. United States*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/ [https://perma.cc/8T9H-Q7MV].

This Comment examines the Sixth Circuit's recent decision in *Carpenter* and analyzes the Sixth Circuit's decision within the context of similar court decisions. Part II looks at the facts of the *Carpenter* case, the court's opinion, the law on which it rests, and similar circuit court decisions. Part III considers the effects of the decision, unanswered questions that remain, and the U.S. Supreme Court's opportunity to review the case.

II. THE CASE ITSELF—A LOOK AT *UNITED STATES V. CARPENTER* AND SIMILAR DECISIONS

Before analyzing the effects of the *Carpenter* decision and looking towards future events, this Comment first examines the case itself and the rationale behind the decision.

A. *The Facts of the Case*

Between December 2010 and March 2011, a string of robberies took place at Radio Shack and T-Mobile stores in and around Detroit, Michigan.[11] In April of 2011, police arrested four individuals whom they believed were involved with the robberies.[12] One man confessed to the crimes.[13] During his confession, he described a team of other individuals who were involved in the criminal activities.[14] This man also gave the FBI his phone and provided the FBI with the phone numbers of individuals he claimed were involved in the robberies.[15]

Equipped with this information, the FBI filed three applications with magistrate judges in an effort to procure the "transactional records" of up to sixteen different phone numbers from their wireless carriers.[16] The most important information that the FBI requested was "cell site [location] information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]"[17] The magistrate judges granted these applications under the Stored Communications Act (SCA).[18] After the FBI obtained this information, Carpenter (and others) were accused of, and charged with, violating the Hobbs Act, among other things.[19]

---

[11] *Carpenter*, 819 F.3d at 884.

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Carpenter*, 819 F.3d at 884 (second alteration in original) (quoting the FBI's application).

[18] *Id.* The relevant section of the Stored Communications Act (SCA) is found in 18 U.S.C. § 2703(d) (2012). The SCA is discussed *infra* Part II.B.

[19] *Carpenter*, 819 F.3d at 884. The Hobbs Act is found in 18 U.S.C. § 1951. The Hobbs Act outlaws any activity that is considered robbery or extortion that interferes with commerce. *See* United States v. Taylor, 754 F.3d 217, 222 (4th Cir. 2014), *aff'd*, 136 S. Ct. 2074 (2016).

Before the trial, the defendants attempted to exclude the CSLI evidence.[20] They argued that the government collection of the CSLI evidence was a violation of their Fourth Amendment right against unreasonable searches and seizures.[21] They claimed that because the search was not supported by a warrant issued with probable cause, the collection of the records was inappropriate.[22] The district court denied the motion, and the case continued to trial.[23]

At trial, individuals involved in the robberies testified about the strategy used to carry out the crimes.[24] Then, an FBI agent testified about the CSLI the FBI obtained.[25]

The agent explained that CSLI is generated when cell phones connect with radio towers to perform certain tasks—such as placing a call.[26] The cell towers have receptors that project radio signals in certain directions, and the phone connects with a certain signal receptor on each tower.[27] By knowing which tower and which specific signal receptor a cell phone connects with, a third party can discover the area in which the cell phone is located.[28] The specificity of this location information largely depends on the density of the towers—the more towers around the cell phone, the more towers a cell phone can connect with, and, therefore, the location of the phone is more precise.[29] The phone company then stores this information for internal use.[30]

Armed with the defendants' CSLI, the FBI created maps showing the location of the defendants' cell phones at certain time periods.[31] These maps revealed that the defendants were within half a mile to two miles of the robbery locations at roughly the same time the robberies occurred.[32]

After being presented with this information, the jury convicted Carpenter on the Hobbs Act charges, among others.[33] The court sentenced Carpenter to

---

[20] *Carpenter*, 819 F.3d at 884.
[21] *See id.*
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*. at 885.
[26] *Carpenter*, 819 F.3d at 885.
[27] *Id.*
[28] *Id.* For example, if I use my cell phone while driving down the highway, my cell phone will connect to Tower A, the closest tower to my cell phone. Assume the highway is south of Tower A. My cell phone will connect to the signal receptor that faces south. Thus, a third party knowing that I was connected to Tower A using the south receptor knows the area where I was when I used my cell phone. *See id.* If, as I drive down the highway, I get closer to Tower B, my phone will connect to Tower B. If I connect with the north signal receptor on Tower B, the third party now knows the area where my cell phone is located (close and north to Tower B). *See id.* With these two data points put together, a third party can also tell the direction in which I am driving.
[29] *See id*.
[30] *Id*.
[31] *Id*.
[32] *Carpenter*, 819 F.3d at 885.
[33] *Id.*

1,395 months of imprisonment, and he and another defendant appealed their convictions and sentences to the Sixth Circuit Court of Appeals.[34]

B. *The Court's Decision and the Legal Ground on Which It Stands*

In an opinion written by Judge Kethledge, the Sixth Circuit found that the collection of the CSLI without a probable cause warrant was not a violation of the defendants' Fourth Amendment rights.[35] The decision is important because it further extends the address/content distinction to a technology driven world.

Traditionally, the Fourth Amendment has been a physical, property based right.[36] However, ever since *Katz v. United States*, the Fourth Amendment framework has focused on the privacy of people, not places and property.[37] After *Katz*, the pertinent question for a Fourth Amendment analysis is: did the government action violate the defendant's "reasonable expectation of privacy."[38]

Due to the ambiguous nature of an individual's reasonable expectation of privacy, courts have developed benchmarks to help determine when an individual has a reasonable expectation of privacy.[39] As the Sixth Circuit points out, one such benchmark is the address/content distinction.[40]

The address/content distinction helps identify privacy protection based on the *type* of information that the government recovers.[41] Address information is information that must be provided to a third party intermediary to complete

---

[34] *Id.*

[35] *Id.* at 890. It should be noted that Congress created a statutory scheme to deal with the recovery of certain electronic information held by companies: the SCA. *See* 18 U.S.C. §§ 2701–2711 (2012). This statute allows a government actor to obtain electronic records with a "less-than-a-warrant standard." Orin Kerr, *6th Circuit: No Fourth Amendment Rights in Cell-Site Records*, WASH. POST: VOLOKH CONSPIRACY (Apr. 13, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/04/13/6th-circuit-no-fourth-amendment-rights-in-cell-site-records/?utm_term=.ab29ec342e52 [https://perma.cc/87K4-EY2L]. In this case, the FBI complied with the statutory scheme. *See Carpenter*, 819 F.3d at 884. The specific challenge in *Carpenter* is that the Fourth Amendment applies to CSLI, and, therefore, the "less-than-a-warrant standard" does not clear the constitutional rigor of the Fourth Amendment. Kerr, *supra*; *accord Carpenter*, 819 F.3d at 884–85. The defendants claim the additional protection of the Fourth Amendment should apply to CSLI, and thus, the standard to retrieve CSLI should be a Fourth Amendment standard and not a Stored Communications Act standard. *See id.* The implications of this distinction are significant. Perhaps most importantly, the exclusionary rule does not apply to violations of the SCA. *See* United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1548 (2015).

[36] *Carpenter*, 819 F.3d at 886.

[37] Katz v. United States, 389 U.S. 347, 351 (1967) ("For the Fourth Amendment protects people, not places."); *see also Carpenter*, 819 F.3d at 886.

[38] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[39] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2008).

[40] *Carpenter*, 819 F.3d at 886.

[41] *See id.*; *see also Forrester*, 512 F.3d at 509–11.

communication.[42] Content information is the actual substance of the message.[43] The Sixth Circuit traces this distinction back to an 1878 case, *Ex Parte Jackson*.[44]

In *Ex Parte Jackson*, the Supreme Court found that the Fourth Amendment protects letters and packages from unreasonable government searches and seizures.[45] However, the Court also found that the outside of letters and packages are not constitutionally protected.[46] The distinction is this: One type of information is addressing information that the sender knows must be seen by a third party intermediary.[47] The other type of information is content information that the sender does not expect the third party intermediary to see.[48] This distinction has remained over time and been applied to new technologies.

The Sixth Circuit then explains the progression of the address/content distinction and discusses instances when courts have applied it to new technologies. Prominently, the court points out that *Katz* itself is about address and content information.[49] In *Katz*, the Supreme Court held that the government could not eavesdrop on the content of a conversation because the conversation was constitutionally protected.[50] However, only twelve years later, the Supreme Court found that the numbers dialed by a phone user were *not* constitutionally protected.[51] The distinction is that the caller must have known that a third party (the phone company) sees the numbers to connect the call.[52] However, the caller does not expect that the substance of the call is recorded or heard.[53]

The Sixth Circuit then discusses the application of the address/content distinction in the digital age.[54] The court refers to its own decision in *United States v. Warshak*.[55] In *Warshak*, the Sixth Circuit held that the content of an email is protected, even though the sender exposes the message to a third

---

[42] *Carpenter*, 819 F.3d at 886; *see also Forrester*, 512 F.3d at 509–11.

[43] *Carpenter*, 819 F.3d at 886; *see also Forrester*, 512 F.3d at 509–11.

[44] *Carpenter*, 819 F.3d at 886 (discussing *Ex Parte* Jackson, 96 U.S 727 (1878)).

[45] *Ex Parte* Jackson, 96 U.S. at 733.

[46] *Id.*

[47] *See Carpenter*, 819 F.3d at 886; *see also Ex Parte* Jackson, 96 U.S. at 733.

[48] *See Carpenter*, 819 F.3d at 886; *see also Ex Parte* Jackson, 96 U.S. at 733.

[49] *Carpenter*, 819 F.3d at 886–87 (discussing Katz v. United States, 389 U.S. 347 (1967)).

[50] *Katz*, 389 U.S. at 353.

[51] Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (discussed in *Carpenter*, 819 F.3d at 887).

[52] *See id.* at 742 ("[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. 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.").

[53] *Id.* at 743.

[54] *Carpenter*, 819 F.3d at 887. For an argument of why the address/content distinction has been misapplied in, and is not fit for, the digital age, see Stevenson, *supra* note 9, at 157–61.

[55] *Carpenter*, 819 F.3d at 887 (discussing United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)).

party.[56] The court reached this conclusion because it sees the email as the modern day letter,[57] and if the contents of a letter are protected, then the contents of an email should also be protected.

The *Carpenter* court follows the logical progression of address/content jurisprudence and applies the same analysis to a new technology: CSLI.[58] Thus, the court analyzed CSLI using the address/content distinction.[59]

It seems clear to the court that CSLI is simply "address" information needed to complete a phone call.[60] When a phone user wants to place a call, companies use CSLI to facilitate the connection of the call through the wireless carrier. The court believes CSLI is similar to the address information in *Ex Parte Jackson* or the phone numbers obtained in *Smith*.[61] On each of these occasions, the recovered information simply facilitates the communication, as opposed to being the substance of the communication. Thus, CSLI is simply address information, which courts have continually held lacks constitutional protection.

The court concludes its argument by asserting that CSLI is voluntarily conveyed to the phone companies.[62] Phone users surely must understand that when they place a call they "expose" their location to the nearest cell phone tower.[63] Further, as the court points out, users must understand that wireless carriers record this information because roaming charges are placed on accounts when the user is out of network.[64] This undercuts the argument that cell phone

---

[56] *Warshak*, 631 F.3d at 288. Although, unlike regular mail and phone calls, the content of an email is exposed to a third party. It can be argued that *Warshak* should not have applied the address/content distinction as it conflicts with the third party doctrine. Thus, even though the substance of an email is content, it should not receive Fourth Amendment protection. *See* Stevenson, *supra* note 9, at 159–60.

[57] *Id.* at 285–86. However, some believe that email is more closely analogous to sending a postcard through the mail because, unlike a letter in an envelope, sending an email allows the third party intermediary to see the contents of the message, like a postcard. *See* NANCY FLYNN & RANDOLPH KAHN, E-MAIL RULES 173 (2003) ("The common analogy is that standard e-mail is like sending a 'postcard written in pencil through the postal mail.' A postcard, because anyone who sees the message along the way can freely read it . . . .").

[58] *Carpenter*, 819 F.3d at 887–88. *Carpenter* may be critiqued for the fact that some believe we should *not* be using the same thought processes to analyze Fourth Amendment challenges in the digital age. *See, e.g.*, *id.* at 894 (Stranch, J., concurring in part) ("The addition of cellular (not to mention internet) communication has left courts struggling to determine if (and how) existing tests apply or whether new tests should be framed. I am inclined to favor the latter approach for several reasons . . . .").

[59] *Id.* at 887–88 (majority opinion) ("Thus, for the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here. On this point, *Smith* is binding precedent.").

[60] *Id.* ("[T]he defendants' cellphones signaled the nearest cell towers . . . solely 'as a means of establishing communication.'" (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979))).

[61] *See supra* notes 47–48, 52 and accompanying text.

[62] *Carpenter*, 819 F.3d at 888.

[63] *Id.*

[64] *Id.*

users are not voluntarily transferring their information to the phone companies when using a cell phone.[65]

C. *Comparing the Decision to Other CSLI Cases*

The *Carpenter* decision may become known not for its novelty, but for its uniformity. The decision helps grow a consensus of courts deciding that there is no reasonable expectation of privacy in CSLI. When the Sixth Circuit issued its opinion, it joined the Fifth[66] and Eleventh[67] Circuits in not protecting CSLI. Shortly thereafter, the Fourth Circuit[68] joined this group.[69]

These circuits all analyzed CSLI under the same framework. They all treated CSLI as business records that are subject to the address/content distinction.[70] Further, all the circuits have compared CSLI to the phone numbers an individual dials when placing a phone call, thus heavily relying on the precedent in *Smith*.[71] This simple, consistent analysis is almost as important as

---

[65] The argument that cell phone users do not voluntarily provide their information in today's technological world has been rejected in other circuits. *See* United States v. Graham, 824 F.3d 421, 429–30 (4th Cir. 2016) (addressing and rejecting the defendant's argument that they did not voluntarily provide their CSLI to phone providers). *But see* United States v. Graham, 796 F.3d 332, 356 (4th Cir. 2015) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." (quoting City of Ontario v. Quon, 560 U.S. 746, 760 (2010))), *adhered to in part en banc*, 824 F.3d 421.

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

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

[68] *See Graham*, 824 F.3d 421.

[69] Interestingly, while the circuits have thus far agreed amongst each other with the treatment of CSLI, one circuit internally disagreed with the treatment of CSLI. The Fourth Circuit originally decided that CSLI was constitutionally protected, *Graham*, 796 F.3d at 349, but that decision was later overturned on an en banc appeal, *Graham*, 824 F.3d 421. In its original decision, the Fourth Circuit panel majority was concerned with how much information can be aggregated when the government collects CSLI. *Graham*, 796 F.3d at 357 ("[S]ociety recognizes an individual's privacy interest in her movements over an extended time period . . . ."). This issue is addressed *infra* Part III.B.

[70] *Graham*, 824 F.3d at 433 ("The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content. CSLI, which identifies the equipment used to route calls and texts, undeniably belongs in the non-content category." (footnote omitted)); *Davis*, 785 F.3d at 515 ("Because Davis has no reasonable expectation of privacy in the type of non-content data collected in MetroPCS's historical cell tower records, neither one day nor 67 days of such records, produced by court order, violate the Fourth Amendment."); *Historical Cell Site Data*, 724 F.3d at 612 ("[T]he historical cell site information reveals his location information for addressing purposes, not the contents of his calls.").

[71] *See Graham*, 824 F.3d at 427; *Davis*, 785 F.3d at 512; *Historical Cell Site Data*, 724 F.3d at 612; *see also* Smith v. Maryland, 442 U.S. 735, 742 (1979).

the holding itself, for courts could analyze the collection of CSLI information using different methods.

No circuit has analyzed the collection of CSLI as a location tracking case. Generally, a different analysis applies when the government actively collects tracking information—such as from the monitoring of movements from a GPS—as opposed to retrieving business records.[72] This distinction is important, as it could lead to a different result.

When the government collects CSLI, it is obtaining snapshots of an individual's location. Many of these snapshots together can create an overview of an individual's movements over time. Thus, it is reasonable to think of CSLI as a location tracking case.[73]

However, every circuit has distinguished CSLI from a location tracking case because cell phone users volunteer their CSLI to a third party for business records as opposed to a location tracking case where the government usually is actively tracking an individual with GPS systems.[74] In other words—tracking is an unwanted government intrusion; CSLI recovery is the government collection of third party records provided by an individual. Therefore, all of the circuits analyze CSLI through a business records analysis instead of a location tracking analysis.

However, the Sixth Circuit also focused on another difference between location tracking and business records: the precision of GPS compared to CSLI.

---

[72] In his opinion in *Carpenter*, Judge Stranch illustrated this distinction when discussing the difficulty in devising a Fourth Amendment test:

> This difficulty is exemplified by the two conceptual categories under the Fourth Amendment found in this case and the law that governs each. The majority accurately describes two different strains of law, one addressing the distinction between GPS tracking and the less accurate CSLI obtained and used in this case and the other "between the content of a communication and the information necessary to convey it."

United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (Stranch, J., concurring in part) (quoting *id.* at 883 (majority opinion)).

[73] *Id.* at 895 ("[I]t seems to me that the business records test is ill suited to address the issues regarding personal location that are before us. I therefore return to the law governing location.").

[74] *Id.* at 889 (majority opinion) (referring to secret GPS tracking by the government, the court noted "[t]hat sort of government intrusion presents one set of Fourth Amendment questions; government collection of business records presents another"); *Graham* 824 F.3d at 426 ("No government tracking is at issue here. Rather, the question before us is whether the government invades an individual's reasonable expectation of privacy when it obtains, from a third party, the third party's records, which permit the government to deduce location information."); *Davis*, 785 F.3d at 513–15 (distinguishing United States v. Jones, 565 U.S. 400 (2012), a GPS tracking case, from the CSLI case that was before the court); *Historical Cell Site Data*, 724 F.3d at 610 ("[T]he Government, when determining whether an intrusion constitutes a search or seizure, draws a line based on whether it is the Government collecting the information . . . or whether it is a third party, of its own accord and for its own purposes, recording the information.").

CSLI, the Sixth Circuit contends, provides much more general information about an individual's location compared to GPS.[75] GPS can locate an individual accurately within fifty feet, whereas CSLI can only "locate" an individual within an area as large as 3.5 million to 100 million square feet.[76] Because the area of CSLI is much broader, the court argues that CSLI is much less invasive than GPS.[77] Many shops, offices, and restaurants fall within the CSLI range, whereas GPS reveals specific shops, offices, and restaurants.[78] This specificity, the court argues, is a major reason to separate a GPS tracking case from a business records case like CSLI.[79]

The Fifth, Eleventh, and Fourth Circuits placed less emphasis on the precision of CSLI as compared to GPS.[80] Rather, the thrust of each circuit's Fourth Amendment analysis focused on individuals voluntarily providing their CSLI to third parties.[81]

The common emphasis among circuits is that the government does not actively track an individual to obtain their CSLI. Rather, the government simply obtained location information from a third party who held the records.[82] This uniform reasoning represents a growing consensus among the circuits on how to treat CSLI. However, this is something to watch in the future, as a location based CSLI framework could lead to a much different result.

III. EXAMINING THE IMPACT OF THE DECISION MOVING FORWARD

Understanding the growing consensus of circuit court decisions, we can now look to the future and examine the implications.

A. *The Decision's Effects on Daily Privacy*

The obvious implication stemming from *Carpenter* is that CSLI for individuals within the Sixth Circuit is not protected under the Fourth

---

[75] *Carpenter*, 819 F.3d at 889.

[76] *Id.* The court notes that this is roughly 12,500 times less accurate than GPS data. *Id.*

[77] *Id.*

[78] *Id.* The court points out that this large of an area could include "bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque." *Id*.

[79] *See id.* at 889–90. The decision of the Sixth Circuit to focus on this specificity is curious. *See infra* Part III.B.

[80] While these circuits did comment on the less precise nature of CSLI as compared to GPS, this was not a central component of their Fourth Amendment analysis. *See generally* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc); United States v. Davis, 785 F.3d 498 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

[81] *See supra* note 74 and accompanying text.

[82] *See supra* note 74 and accompanying text. *Carpenter* did not ignore this reality. *Carpenter*, 819 F.3d at 889. The underlying idea of the address/content distinction is that the address information is willingly provided to a third party.

Amendment. This means that every time an individual places a phone call, the government can retroactively discover the general location of the individual.[83]

The Sixth Circuit decision applies to *historical* CSLI.[84] This means that we do not know if the government can currently request an individual's future CSLI. After *Carpenter*, the government can only request an individual's prior CSLI, as opposed to requesting records for CSLI for the next six months. However, this does not limit the government from submitting a request every month, week, or even day for an individual's CSLI.

In fact, other than knowing the government can request historical CSLI, *Carpenter*'s implications on daily privacy are ambiguous at best. This is because the Sixth Circuit's decision left many important, tangential CSLI questions unanswered.

B. *Unanswered Questions—What the Sixth Circuit Didn't Say*

As Fourth Amendment doctrine develops with new technology, the questions that the Sixth Circuit left unanswered in *Carpenter* are extremely important to courts and individuals alike. Specifically, after *Carpenter* it is unknown how the Sixth Circuit will treat 1) non-phone call generated CSLI, 2) more precise CSLI, 3) third party GPS cases, and 4) mass amount of information cases.

1. *Non-Phone Call Generated CSLI*

In *Carpenter*, the FBI search applications specifically requested CSLI generated from a specific event: the defendants actively placing a call.[85] However, with advancements in cellular devices, phones now send text messages, use GPS for certain applications, and much more. Each event that generates CSLI creates another specific event that the government can then request from a wireless carrier.[86] Further, cellular devices are constantly emitting radio waves attempting to find the nearest cell tower, and thus, are constantly generating CSLI.[87]

---

[83] *See* Meyer, *supra* note 6.

[84] *Carpenter*, 819 F.3d at 889 ("*Jones*, in contrast, lands near the other end of the spectrum: there, government agents secretly attached a GPS device to the underside of Jones's vehicle and then monitored his movements *continuously* for four weeks. That sort of government intrusion presents one set of Fourth Amendment questions; government collection of business *records* presents another." (emphasis added)).

[85] *Id.* at 884.

[86] *See* United States v. Davis, 785 F.3d 498, 542 (11th Cir.) (Martin, J., dissenting) ("[T]oday, the vast majority of communications from cell phones are in the form of text messages and data transfers, not phone calls."), *cert. denied*, 136 S. Ct. 479 (2015).

[87] *Carpenter*, 819 F.3d at 885 ("[C]ellphones work by establishing a radio connection with nearby cell towers (or 'cell sites'); . . . phones are constantly searching for the strongest signal from those towers . . . ."); *Davis*, 785 F.3d at 542 (Martin, J., dissenting) ("As a person walks around town, particularly a dense, urban environment, her cell phone continuously

The Sixth Circuit, and the other circuits, all base their decisions on the business records and address/content distinctions.[88] These doctrines are based on a user voluntarily exposing information to a third party intermediary.[89] However, at what point does voluntary disclosure cease to apply?[90]

In the case of specific cellular events, such as a phone call or text message, we probably have our answer: never. The logical extension of *Carpenter* is that any time a specific attempt to communicate via cell phone occurs, the transfer of information is voluntary. However, what happens when there is no attempt at communication, and a user's phone is simply sitting in a pocket or on a table?

In today's world, ownership of a cell phone is almost necessary. Cellular calls, text messages, email, mobile banking, directions, and much more are all features of a modern cell phone. It would be almost unthinkable to not have a cell phone in the digital world that we live in today.[91]

Because cellular devices are constantly emitting radio waves to locate radio towers, CSLI is constantly generated.[92] Does the act of carrying a cellular device constitute a voluntary conveyance of one's location to a third party? Will the government be able to request records for CSLI when the phone is simply sitting idle in the user's pocket?[93] We do not know the answers to these questions, but if we extend the logic of *Carpenter* and other CSLI cases, the result does not look good for privacy.

---

and without notice to her connects with towers, antennas, microcells, and femto-cells that reveal her location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot. And since a text or phone call could come in at any second—without any affirmative act by a cell phone user—a user has no control over the extent of location information she reveals.").

[88] *See supra* note 70 and accompanying text.

[89] In *Smith* (which the Sixth Circuit relies on heavily to emphasis the address/content distinction), the Court stated: "[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." Smith v. Maryland, 442 U.S. 735, 744 (1979).

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

[91] *Davis*, 785 F.3d at 539 (Martin, J., dissenting) ("Today, 'it is the person who is not carrying a cell phone . . . who is the exception.'" (alteration in original) (quoting *Riley*, 134 S. Ct. at 2490)).

[92] *See supra* note 87; *see also Davis*, 785 F.3d at 542 (Martin, J., dissenting) ("'[S]martphones . . . communicate even more frequently with the carrier's network, because they typically check for new email messages or other data every few minutes.' . . . Each of these new types of communications can generate cell site location data." (quoting ACLU amicus brief)). In the *Davis* case, a dissenting opinion pointed out that the government obtained 11,606 CSLI data points over sixty-seven days. *Id.* at 533. If the court assumes the defendant slept for eight hours a day, this corresponds to one data point being generated every five and a half minutes. *Id.* at 540.

[93] When a smartphone sits idly in a pocket, it can still generate CSLI by providing some smartphone services for the user, such as checking email. *See supra* note 92 and accompanying text.

When an individual buys a phone and wants cellular service, a user signs a contract with a wireless company to use its network. Following the logic of the Sixth Circuit, this contract may be considered voluntary consent to provide the phone company with their location as long as they are connected to the wireless carrier's network, even if not actively using their phone.[94] That CSLI will become a "business record," and thus lose all Fourth Amendment protection.

2. *More Precise CSLI Cases*[95]

Each circuit that has addressed CSLI has mentioned the relative generality of location information revealed by CSLI.[96] The Sixth Circuit (for curious reasons) showed a particular interest in this generality compared to GPS location information.[97] However, the generality of CSLI may soon be a relic of the past.

The denser the cellular tower network, the more specific the CSLI will be.[98] With the number of cellular sites rapidly increasing (and showing no signs of slowing down), CSLI is certain to be much more precise in the future.[99] If an important consideration for Fourth Amendment protection is truly the generality of CSLI, at what point does CSLI become more concerning to the courts? Is it when CSLI can pinpoint location within one mile? Five hundred feet? Ten feet? We do not hold the answer to this question. But again, if we follow the logic of *Carpenter*, these specifics will not matter.[100]

---

[94] *See* United States v. Graham, 824 F.3d 421, 430 (4th Cir. 2016) (en banc) ("A cell phone user voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function. Whenever he expects his phone to work, he is permitting—indeed, requesting—his service provider to establish a connection between his phone and a nearby cell tower." (citation omitted)).

[95] It should be noted that the Sixth Circuit explicitly sidestepped this problem in their decision. The court decided not to address arguments regarding "femtocells" that can locate a phone within ten meters. United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) ("[O]ur task is to decide this case, not hypothetical ones; and in this case there are no femtocells to be found.").

[96] *See Graham*, 824 F.3d at 447 (Wynn, J., dissenting in part and concurring in the judgment); *Davis*, 785 F.3d at 515; *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 609 (5th Cir. 2013).

[97] *See supra* notes 75–79 and accompanying text.

[98] *Davis*, 785 F.3d at 542 (Martin, J., dissenting) ("As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced . . . ." (quoting ACLU amicus brief)). This is why urban CSLI is more precise than rural CSLI. *Id.* at 503 (majority opinion) ("[T]he density of cell towers in an urban area like Miami would make the coverage of any given tower smaller.").

[99] The number of cell sites has almost doubled in the past decade, and phone companies are always attempting to upgrade their service by improving their networks with more cell towers. *Id.* at 541–42 (Martin, J., dissenting).

[100] A dissenting judge in *Graham* alluded to this:

> [A] narrower holding would have allowed this Court to grapple, in the future, with the effect of rapidly changing phone technology, like the increasing "proliferation of

Even if CSLI could pinpoint location down to the millimeter, the central premise of *Carpenter* remains: an individual volunteered that information to a business.[101] It is simply address information the company uses to complete a communication. Thus, following the logic in *Carpenter*, protection even for the most precise locations will remain unprotected. However, this runs counter to one of the Sixth Circuit's main arguments: CSLI does not reveal intimate details like GPS tracking does. These two competing rationales will eventually come to a head, and we do not know which will prevail.

3. *GPS Third Party Business Records*

Similar to the increasingly precise CSLI concern is the use of current GPS third party records. These are tools such as Google Maps[102] or the GPS systems in cars. These types of tools use GPS data to provide directions for users going from point A to point B. It is important to note—third parties provide these tools only to users who volunteer their location information by inputting information to use the service.

The location information held by these companies runs into the same problem as more specific CSLI: the information is very revealing, but it is still a business record. Therefore, will courts focus on the specificity of information and protect this location information by treating it like a GPS tracking case? Or, will courts place more emphasis on the voluntary disclosure of information to a third party, and treat this like a CSLI case that loses any expectation of privacy?

We are unsure how courts will handle this moving forward. However, following the rationale of *Carpenter*, this information is a business record and will be subject to the address/content distinction.

Assuming courts use the address/content distinction in this scenario, another problem arises: with these types of services, the address information *is* the content information. The location of the user is the information needed to complete the service (i.e., the phone numbers revealed in *Smith*, or the address in *Ex Parte Jackson*). However, a court could also consider that information the content of the service—the substance of the service is to provide geographic information to the user.

> smaller and smaller [cell sites] such as microcells, picocells, and femtocells—which cover a very specific area" . . . . Rather, the majority concedes what follows unavoidably from its holding: "the applicability of the Fourth Amendment [does not] hinge[ ] on the precision of CSLI," or on its quantity.

Graham, 824 F.3d at 448 (Wynn, J., dissenting in part and concurring in the judgment) (alterations in original except "[A]") (citations omitted) (first quoting *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015); and then quoting *Graham*, 824 F.3d at 426 n.3 (majority opinion)).

[101] *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

[102] Google Maps is a smartphone application that provides users with driving, walking, or transit directions. *See About*, GOOGLE MAPS, https://www.google.com/maps/about/ [https://perma.cc/Y3WZ-6AC4].

After *Carpenter*, we do not know how courts will treat this information. Will they protect the information because it is extremely specific and revealing? Will they not protect the information because it was voluntarily provided to a business? Will they use the address/content distinction, and if they do, is the data classified as address or as content information? The framework the Sixth Circuit adopts in *Carpenter* leaves all these questions unanswered.

4. *Mass Amounts of Information*

Last but not least, the Sixth Circuit (nor the other circuits) did not limit how much CSLI the government can obtain. In *Carpenter*, the FBI collected 127 days' worth of CSLI.[103] However, under the current framework, what stops the FBI from collecting more?

If location information loses Fourth Amendment protection because it is a business record, nothing stops the FBI from collecting as much CSLI as the third party has on record.[104] This could lead to the FBI requesting six months, two years, or even decades' worth of location information.[105] It is hard to imagine an America where the government can access a decade's worth of location information without a search warrant. However, that is exactly the door that *Carpenter* opens.[106]

C. *The Supreme Court's Opportunity to Protect Privacy*

With all these questions in mind, the Supreme Court now has the opportunity to review *Carpenter*, and more importantly, the role of the Fourth Amendment in the digital world. The Supreme Court should not sidestep this opportunity.[107]

---

[103] *Carpenter*, 819 F.3d at 886. 127 days can provide an absurd amount of geographic data points. In another case, sixty-seven days provided over 11,000 data points. *See supra* note 92.

[104] *See Carpenter*, 819 F.3d at 896 (Stranch, J., concurring in part) ("I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled.").

[105] These long time frames are unlikely because the SCA requires this type of information to be connected to a reasonable belief of criminal activity. *See* United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015), *adhered to in part en banc*, 824 F.3d 421 (4th Cir. 2016). It is hard to believe a court would grant permission for the government to obtain information for that long of a time period. However, imagine a drug ring or financial crime that has occurred over a lengthy period of time. Nothing will stop the government from accessing these individuals' location information for the entire time period.

[106] One solution to this problem is the adoption of the mosaic theory. For a discussion of the mosaic theory, see generally Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012). To see how courts could use the mosaic theory in conjunction with the third party doctrine, see Stevenson, *supra* note 9, at 161–63.

[107] The Supreme Court already passed on the opportunity once when it denied certiorari for the *Davis* case. *Davis v. United States*, SCOTUSBLOG, http://www.scotusblog .com/case-files/cases/davis-v-united-states-2/ [https://perma.cc/XH96-VD5W].

If the Supreme Court reviews *Carpenter* and upholds the Sixth Circuit's decision, the Supreme Court will still provide necessary guidance to lower courts dealing with CSLI issues. The Court will either agree with the growing consensus on CSLI, or it will instruct the lower courts to analyze CSLI differently (such as a location tracking analysis). However, it may be more prudent for the Supreme Court to review *Carpenter* and use the platform to offer its vision for the future of Fourth Amendment jurisprudence.

Because of rapidly changing technology, the time is ripe for a new approach to Fourth Amendment cases. The Supreme Court could begin those changes with a review of *Carpenter*.

With a review of *Carpenter*, the Court could do many things. First, the Court could take a traditional stance on the third party doctrine and reinforce that even during the digital age, anything provided to a third party is not protected. Second, the Court could abandon the third party doctrine, because it is not suitable for the twenty-first century. Third, the Supreme Court could adopt a compromise approach that preserves the third party doctrine, but also recognizes privacy for the digital world in which we live.[108] Fourth, the Court could more clearly articulate the standard for when a location based analysis applies and when a business records, address/content distinction analysis applies.

This list is by no means exhaustive; the avenues available for the Court to update the Fourth Amendment are almost limitless.

IV. CONCLUSION

After *United States v. Carpenter*, only one thing is clear: cell phone users in the Sixth Circuit do not have Fourth Amendment protection over their CSLI. The Sixth Circuit issued a sound—albeit safe—opinion applying traditional Fourth Amendment principles to new technology. Unfortunately, applying traditional principles leaves many questions unanswered. More importantly, applying these traditional principles may also diminish the privacy individuals should enjoy in the future.[109]

The action now moves to the Supreme Court, which has the opportunity to review *Carpenter*. If the Supreme Court reviews the case, it can examine the Fourth Amendment and determine how it will operate in the twenty-first century. Or, the Supreme Court can choose to not review the case, and continue to ignore the almost guaranteed privacy issues that will only worsen if traditional thinking is applied to untraditional technology.

---

[108] For one example of how the Supreme Court can attempt to strike this balance, see generally Stevenson, *supra* note 9.

[109] Discussing the Fourth Circuit's application of traditional principles from *Miller* and *Smith*, a dissenting judge stated: "In other words, the majority's expansive interpretation of *Miller* and *Smith* will, with time, gather momentum—with effects increasingly destructive of privacy." United States v. Graham, 824 F.3d 421, 446 n.8 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in the judgment).