CARPENTER V. UNITED STATES: HOW MANY CELL PHONE LOCATION POINTS CONSTITUTE A SEARCH UNDER THE FOURTH AMENDMENT?

DOUGLAS HARRIS*

INTRODUCTION

Did you know that cell-phone service providers collect and store your location data every time you place or receive a phone call? Your answer to this question may impact how the Supreme Court views the warrantless search and seizure of cell phone records, including the location and movement of the user, under current Fourth Amendment jurisprudence.

Using a cell phone would not be possible without the existence of cell towers or "cell sites." Cell phones have to connect to nearby cell towers with the best signal to access the cellular network and make a call. Cellular service providers record which cell sites are used when a customer starts and ends a phone call, thereby creating cell site location information ("CSLI"). "The precision of a cell phone user's location reflected in CSLI records depends on the size of the cell site 'sectors' in the area"; when there are more antennas on the cell site, there are more sectors. Areas with the most cell sites and the smallest sectors, like urban metropolitan areas, make the CSLI data pertaining to a user's potential location within the sector more accurate.

Copyright © 2018 Douglas Harris.

^{*} J.D. Candidate, Duke University School of Law, Class of 2019.

^{1.} Brief for Petitioner at 14, Carpenter v. United States, 2017 WL 3575179 (2017) (No. 16-402) [hereinafter Brief for Petitioner].

^{2.} *Id.*; see also Brief for Respondent at 10, Carpenter v. United States, 2017 WL 4311113 (2017) (No. 16-402) [hereinafter Brief for Respondent].

^{3.} Brief for Respondent, *supra* note 2, at 14.

^{4.} *Id*.

^{5.} *Id.* at 14–15.

In Carpenter v. United States, 6 the Supreme Court must decide whether the government's acquisition of a suspect's CSLI records during an ongoing criminal investigation is a "search" under the Fourth Amendment, and thus requires a showing of probable cause to obtain a warrant. Petitioner, Timothy Carpenter, used his cell phone before and after robbing multiple stores in the Detroit area. Cell sites covered areas in Detroit ranging from half a mile to two miles.8 When assessing whether the government was legally entitled to gather his CSLI records, the Court must account for a 1986 statute, the Stored Communications Act.9 The statute carves out an exception for accessing such records—the governmental entity must only show "reasonable grounds" during an ongoing criminal investigation to obtain a court order.¹⁰ The Court must rely on various tests concerning business records, property-based analyses, and reasonable expectations of privacy to come to a decision. Thus, the Court's opinion may hinge on a reasonable person's answer to the question opening this Commentary.

Although this opinion will have future consequences for Americans and their privacy interests as cell sites continue to be built and CSLI records increasingly contain more private information, 11 this Commentary argues that the necessity of owning and using cell phones renders past tests obsolete. With wavering, subjective expectations of what information is actually private in society today, the Court should thus create a new test that makes a prescriptive claim about expectations of privacy and compares newer technologies with older ones. The Court should then hold that obtaining CSLI records without a warrant is an unreasonable search under the Fourth Amendment.

I. FACTS

Petitioner, Timothy Carpenter, was convicted of committing a series of armed robberies at several Radio Shack and T-Mobile stores throughout Michigan and Ohio from December 2010 to March 2011.¹²

^{6. 137} S. Ct. 2211 (2017).

^{7.} United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016).

^{8.} *Id*

^{9. 18} U.S.C. § 2703(d) (2012).

^{10.} Id.

^{11.} Brief for Petitioner, *supra* note 1, at 15.

^{12.} Brief for Respondent, *supra* note 2, at 13.

In April 2011, police arrested four individuals involved in the crimes. ¹³ One of the individuals confessed that he was a part of a group of fifteen men—"a shifting ensemble of . . . getaway drivers and lookouts"—that robbed nine stores. ¹⁴ The confessor gave the FBI all participants' cellphone numbers. ¹⁵

In May and June 2011, the FBI submitted three orders to magistrate judges for "transactional records" from wireless cellphone carriers for sixteen different phone numbers. 16 In addition to a list of numbers called and received, the FBI requested "cell site information" for the target telephones at call origination and at call termination for incoming and outcoming calls" beginning on December 1, 2010. The FBI stated that these records would provide evidence that Petitioner and others violated the Hobbs Act, 18 U.S.C. § 1951. 18 The magistrates granted the requests pursuant to the Stored Communications Act, ¹⁹ which allows courts to issue orders when "the governmental entity offers specific and articulable facts showing that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."²⁰ MetroPCS turned over 127 days of cell-site records²¹ including 186 pages of Carpenter's cell phone records showing the cell site and sector at the start and end of his phone calls.²²

Although MetroPCS was Petitioner's primary provider, the company did not have coverage in one of the areas the charged robberies took place.²³ When Petitioner was in that area, his phone began to use Sprint's cell towers since MetroPCS had a roaming agreement with Sprint that increased MetroPCS customers' coverage

^{13.} United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016), cert. granted, 137 S. Ct. 2211 (2017).

^{14.} *Id*.

^{15.} *Id*.

^{16.} *Id*.

^{17.} *Id*.

^{18.} *Id.*; see also 18 U.S.C. § 1951 (2012) ("Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.").

^{19. 18} U.S.C. § 2703.

^{20.} Id. § 2703(d); Carpenter, 819 F.3d at 884.

^{21.} Brief for Respondent, supra note 2, at 14.

^{22.} Brief for Petitioner, *supra* note 1, at 19.

^{23.} *Id.* at 20.

area.²⁴ Sprint thus provided two days of cell site location information.²⁵ In total, the government accessed 12,898 CSLI data points, an average of 101 points per day.²⁶

Petitioner was charged with counts of aiding and abetting robbery that affected interstate commerce in violation of the Hobbs Act, and aiding and abetting the use or carrying of a firearm during a federal crime of violence.²⁷ Before trial, Petitioner moved to suppress the CSLI records "on the basis that the Fourth Amendment prohibits their acquisition without probable cause and a warrant."²⁸ The Eastern Michigan District Court denied Petitioner's motion to suppress the government's cell-site evidence because "people do not have a reasonable expectation of privacy in CSLI records—and, consequently, their acquisition by the government does not constitute a 'search' under the Fourth Amendment."²⁹

At trial, seven accomplices testified that Petitioner organized most of the robberies, supplied the guns, and served as a lookout.³⁰ As an expert witness, an FBI agent testified about the cell-site data and how cell sites in Detroit individually cover areas ranging from a half-mile to two miles.³¹ The agent created maps showcasing how Petitioner's phone was "within a half-mile to two miles of the location of each of the robberies around the time the robberies happened," placing him near the scene of each crime.³²

Petitioner was convicted by a jury on all of the Hobbs Act counts and all but one of the gun counts.³³ He was sentenced to 116 years and 4 months imprisonment.³⁴ The Sixth Circuit affirmed the district court's decision, relying on *United States v. Jones*,³⁵ where five Justices agreed that people have a reasonable expectation of privacy regarding "longer term GPS monitoring in government investigations of most

- 24. See id.
- 25. Brief for Respondent, *supra* note 2, at 15.
- 26. Brief for Petitioner, supra note 1, at 21.
- 27. United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).
- 28. Brief for Respondent, *supra* note 2, at 21.
- 29. Brief for Respondent, *supra* note 2, at 21.
- 30. Carpenter, 819 F.3d at 884.
- 31. Id. at 885.
- 32. *Id*.
- 33. Id.

^{34.} See id. ("Carpenter's convictions on the § 924(c) counts subjected him to four mandatory-minimum prison sentences of 25 years, each to be served consecutively, leaving him with a Sentencing Guidelines range of 1,395 to 1,428 months' imprisonment.").

^{35. 565} U.S. 400 (2012).

offenses."³⁶ The Sixth Circuit distinguished CSLI data from GPS monitoring, held that individuals do not have a reasonable expectation of privacy with CSLI data,³⁷ and further held that this type of collection of business records is not a "search" under the Fourth Amendment.³⁸ Carpenter's petition for a writ of certiorari from the Supreme Court of the United States was granted on June 5, 2017.³⁹

II. LEGAL BACKGROUND

The Fourth Amendment affords individuals a constitutional right to privacy: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause...." Although the Fourth Amendment was originally interpreted to protect citizens from government intrusion into homes, it now "protects people, not places." This wider conception of the Fourth Amendment not limited to physical intrusions came with a "twofold requirement" test: (1) the person must have an actual, subjective expectation of privacy; and (2) "the expectation [must] be one that society is prepared to recognize as 'reasonable." Although Justice Harlan formed this test in his concurring opinion in *Katz v. United States*, the Court has applied his analysis to later cases.

In *Katz*, the Supreme Court held that FBI agents must show probable cause to obtain a warrant for attaching an electronic recording device to a public telephone booth.⁴⁶ In Justice Harlan's analysis, the crucial fact was that a person speaking inside a closed phone booth reasonably assumes that his call is not being

^{36.} Brief for Respondent, *supra* note 2, at 22–23 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

^{37.} *Carpenter*, 819 F.3d at 888.

^{38.} Id. at 890.

^{39.} Carpenter v. United States, 137 S. Ct. 2211 (2017).

^{40.} See U.S. CONST. amend. IV.

^{41.} *Jones*, 565 U.S. at 405 ("Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

^{42.} Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

^{43.} *Id*.

^{44.} Id. at 360.

^{45.} *Jones*, 565 U.S. at 405–06 (citing Bond v. United States, 529 U.S. 334 (2000); California v. Ciraolo, 476 U.S. 207 (1986); Smith v. Maryland, 442 U.S. 735 (1979)).

^{46.} See Katz, 389 U.S. at 355–59.

intercepted.⁴⁷ Twelve years later in *Smith v. Maryland*,⁴⁸ the Court considered whether a warrant was required for the police to request a telephone company to install a pen register at an individual's office.⁴⁹ The pen register would record which numbers were dialed from the individual's home.⁵⁰ The Court applied the *Katz* analysis, stating that telephone users do not have "any actual expectation of privacy in the numbers they dial" because people must "convey phone numbers to the telephone company" to complete the calls.⁵¹ The Court continued by stating that "[a]ll subscribers realize . . . that the phone company . . . make[s] permanent records of the numbers they dial."⁵² For the second part of the test, the Court held that a person has "no legitimate expectation of privacy in information he voluntarily turns over to third parties."⁵³ Nonetheless, the Court maintained that the content of the phone call—the words spoken during the conversation—was private.⁵⁴

Forty-five years after *Katz*, in *United States v. Jones*,⁵⁵ the Court held that the government's attachment of a GPS device on a citizen's vehicle to monitor its movements was a "search" under the Fourth Amendment.⁵⁶ However, Justice Scalia, in writing for the majority, did not apply the *Katz* test because "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation."⁵⁷ Instead, the majority relied on a textual analysis of the Fourth Amendment with an individual's vehicle being an "effect," a term listed along with persons, houses, and papers.⁵⁸ The majority's recapitulation of Harlan's

^{47.} Id. at 361 (Harlan, J., concurring).

^{48. 442} U.S. 735 (1979).

^{49.} Id. at 737.

^{50.} *Id*. at

^{51.} Id. at 742 (quotations omitted).

^{52.} *Id*.

^{53.} *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

^{54.} *See id. at* 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

^{55. 565} U.S. 400 (2012).

^{56.} Id. at 404.

^{57.} Id. at 406.

^{58.} See id. at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment.").

standard from *Katz* was that it should be used in "add[ition] to, not substituted for, the common-law trespassory test." ⁵⁹

In *United States v. Miller*, 60 the Court reiterated that it

held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.⁶¹

This voluntary disclosure of information to third parties diminishes the individual's expectation of privacy, even in the context of a governmental entity obtaining a person's bank records.⁶² The bank records were not "private papers" but were the bank's business records.⁶³ Accordingly, "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."⁶⁴

In addition to addressing the precedential impact of these cases, Carpenter will likely address the Stored Communications Act, 18 U.S.C. § 2703, which states in relevant part that "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity" obtains a warrant or a court order. 65 Although a warrant requires probable cause, 66 the statute allows a court order for disclosure "when the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."67 Thus, the statute allows a "reasonable grounds" standard for accessing certain records from a telephone company. The Stored Communications Act became

^{59.} *Id.* at 409; see also id. at 414 ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the government physically invades personal property to gather information, a search occurs.").

^{60. 425} U.S. 435 (1976).

^{61.} Id. at 443.

^{62.} Id. at 442.

^{63.} Id. at 440.

^{64.} Id. at 443.

^{65. 18} U.S.C. § 2703(c) (2012).

^{66.} FED. R. CRIM. P. 41(d).

^{67. 18} U.S.C. § 2703(d).

effective in 1986, a time where communications records were never as comprehensive as they are today.

III. HOLDING

In Carpenter, the Sixth Circuit affirmed the lower court's decision, holding that the government's collection of CSLI as a request for business records was not a Fourth Amendment search.⁶⁸ The court began its analysis with a brief history of the Fourth Amendment, discussing its historical expansion from a "property-based understanding" to "protect[ing] certain expectations of privacy as well,"69 and the creation of the Katz test to determine what is a "search." Then, the court focused on the content-context distinction that further guides the analysis.⁷¹ In *Katz*, the police could not surveil the content of the conversation taking place in the phone booth without a warrant, nor could the police listen to the conversations in Smith. 72 However, the caller in Smith could not expect the context of his conversation—the phone numbers he dialed—to remain private.⁷³ Although the Sixth Circuit acknowledged that the content of emails are still protected, courts have not extended the same protection to metadata used in sending these internet communications, "like sender and recipient addresses on an email, or IP addresses."74

Based on this precedent, the court found that "the business records here fall on the unprotected side of this line" because CSLI data helped facilitate the personal communications and did not include the actual content of the communications.⁷⁵ Using *Smith*, the court reasoned that cellphone users knew, during a call, they were

^{68.} United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016).

^{69.} Id. at 886.

^{70.} Id.

^{71.} See id. at 883 ("In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it.").

^{72.} *Id.* at 887.

^{73.} See id. ("But in Smith, the Court held that the police's installation of a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private. 'Although [the caller's] conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.'") (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)).

^{74.} See id. (citing United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007)).

^{75.} *Id*.

exposing their location to the nearest cell tower and its respective company because these users saw their "phone[s'] signal strength fluctuate." Additionally, anyone that paid cellphone charges should have expected that these phone companies recorded locational information for "legitimate business purposes." When the Sixth Circuit applied the test from *Katz*, the court emphasized language from *Smith*: "it is important to begin by specifying *precisely the nature of the state activity that is challenged.*" Because the nature of the activity is obtaining business records from a third party, these defendants had a diminished expectation of privacy for the related information.

The Sixth Circuit paid great deference to the legislative intent of the Stored Communication Act, explaining that "[t]he act strikes out a middle ground between full Fourth Amendment protection and no protection at all" with its "reasonable grounds" requirement. This middle ground was constitutional because the second part of the *Katz* test asks if the expectation of privacy "is one that society is prepared to recognize as reasonable. and society, in the form of elected legislators, has "struck a balance that it thinks is reasonable." The majority opinion finally acknowledged the exponential speed at which technology advances, thus making Congress the better body of government to deal with these types of issues.

The Sixth Circuit supplemented their analysis by comparing the case to *Jones*, repeating that the attachment of a GPS device did not concern business records and, thus, deals with a different legal question.⁸⁴ But the court still distinguished the facts at hand from *Jones*, since CSLI is not as accurate as GPS information.⁸⁵ GPS data was accurate within fifty feet but the locational data here was

^{76.} See id. at 888.

^{77.} Id. (citation omitted).

^{78.} Id. (quoting Smith, 442 U.S. at 741) (emphasis in original).

^{79.} Id. at 888-89.

^{80.} Id.

^{81.} Id. at 889–90 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

^{82.} Id. at 890.

^{83.} See id. ("But sometimes new technologies—say, the latest iterations of smartphones or social media—evolve at rates more common to superbugs than to large mammals. In those situations judges are less good at evaluating the empirical assumptions that underlie their constitutional judgments.").

^{84.} See id. at 889 ("That sort of government intrusion presents one set of Fourth Amendment questions; government collection of business records presents another. And the question presented here, as shown above, is answered by Smith.").

^{85.} Id.

"accurate within a 3.5 million square-foot to 100 million square-foot area." The court was also careful to say that Petitioner "lack[ed] any property interest in cell-site records created and maintained by their wireless carriers." 87

Conversely, Judge Stranch's concurrence asserted that approaching the case by focusing on how the information is voluntarily disclosed to third parties "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."88 Judge Stranch conceded that CSLI data was less precise than GPS tracking but used United States v. Skinner⁸⁹ to assert her concern that "longterm location monitoring in government investigations impinges on expectations of privacy."90 The court in Skinner held that the "defendant did not have a reasonable expectation of privacy in the GPS data and the location of his cellphone" when DEA agents tracked him over three days.⁹¹ Judge Stranch was worried that this case reached the territory Justice Alito warned about in Jones: "there may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." The tracking here exceeded Skinner by collecting four months of CSLI data. 92 Judge Stranch argued that the existing tests make the business records containing CSLI data akin to business records containing credit card purchases, which do not reflect personal location to the same degree. 93 Thus, Judge Stranch believed this type of treatment showed the need for a new test.⁹⁴

^{86.} *Id*.

^{87.} Id. at 888.

^{88.} *Id.* at 894 (Stranch, J., concurring) (quoting United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring)).

^{89. 690} F.3d 772 (6th Cir. 2012).

^{90.} Carpenter, 819 F.3d at 895.

^{91.} United States v. Skinner, 690 F.3d 772, 780–81 (6th Cir. 2012).

^{92.} Carpenter, 819 F.3d at 895.

^{93.} See id. at 889 ("In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location.").

^{94.} *Id.* at 896.

IV. ARGUMENTS

In *Carpenter*, Petitioner and the United States disagree about whether the collection of CSLI data pursuant to the Stored Collection Act is constitutional. Namely, the issue is whether a governmental entity can obtain a court order for such information without showing probable cause.

A. Petitioner's Arguments

Petitioner's arguments are grounded in the privacy concern that allowing this warrantless access of CSLI data will result in the government's ability to use this tool to access any citizen's minute-by-minute location. Petitioner's conclusion is supported by (1) using the *Katz* test in union with the similar facts in *Jones* to state that Petitioner had a reasonable expectation of privacy with the CSLI records, (2) supplementing the property-based analysis in using another relevant congressional statute, and (3) downplaying the thrust of the third-party/business records doctrine.

First, Petitioner argued that individuals have a reasonable expectation of privacy with their longer-term cellular location records under the Katz test. Petitioner used language from Jones in his reasonable-expectation-of-privacy calculus, accounting for expectation of privacy against the government prior to the creation of the new technology.⁹⁶ As people expect the government to not secretly monitor the movement of their vehicles, they also expect the same privacy with their longer-term cell phone location records because cell phones are carried almost everywhere people go.⁹⁷ Therefore, before the advent of cell-phones, the government could not intimately track individuals in this manner. 98 Petitioner bolstered his claim of confidentiality with the federal Telecommunications Act, 47 U.S.C. § 222(c)(1), which declared that cell phone providers cannot disclose location data without "approval of the customer."99 Petitioner's worry is exacerbated with future technological advancements likely narrowing the location accuracy gap between

^{95.} See Brief for Petitioner, supra note 1, at 30.

^{96.} See id. at 30–31 ("[T]his Court has stressed that the reasonable-expectation-of-privacy inquiry must 'assur[e] preservation of that degree of privacy against government that existed' prior to the advent of the new technology in question.") (quoting United States v. Jones, 565 U.S. 400, 406 (2012)).

^{97.} *Id.* at 32–34.

^{98.} Id. at 35-36.

^{99.} Id. at 40-41.

GPS and CSLI, especially with more cell sites being constructed in dense areas.¹⁰⁰ Furthermore, CSLI records are expanding and becoming more plentiful in conjunction with cellular service providers collecting and retaining location information when an individual checks a text message, sends an email, and uses apps.¹⁰¹

Second, Petitioner used a property-based analysis to argue that CSLI records constitute protected "papers" under the Fourth Amendment because CSLI data is rendered as "customary proprietary network information" under the federal Telecommunications Act;¹⁰² this information cannot be disclosed "without the express prior authorization of the customer." Accordingly, the statute made CSLI a proprietary interest of the customer as a "paper" or "effect" and therefore, the data is owned by the customer and not the carrier. ¹⁰⁴

Last, Petitioner argued that the premise of the third-party doctrine, the idea that disclosing information to a third party necessarily ensures that the individual cannot reasonably expect the information to be private, is merely a factor to be considered and not a dispositive test. The petitioner claimed that this principle, combined with the recognition that the Fourth Amendment must account for new technology, effectively resolves this case. Therefore, by showing a reasonable expectation of privacy and that this disclosure is a "search" under the Fourth Amendment, the Government must show probable cause to obtain a warrant for CSLI records. The second of the control of

B. The Government's Arguments

In response to Petitioner's argument about third-party disclosure and reasonable expectation of privacy, the Government first argued that Petitioner cannot claim a privacy interest in CSLI records that he

^{100.} Id. at 44-45.

^{101.} Id. at 51.

^{102.} Id. at 57.

^{103. 47} U.S.C. § 222(f) (2012).

^{104.} Brief for Petitioner, supra note 1, at 59.

^{105.} See id. at 74 ("Although it may someday be necessary to 'reconsider the premise' of the third-party doctrine, it is not necessary in this case to reassess its continued validity in every possible context. Properly understood, the disclosure of information to a third party is but one factor in determining whether a reasonable expectation of privacy exists.") (quoting United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring)).

^{106.} Id. at 74-75.

^{107.} Id. at 92.

voluntarily disclosed to his cell-service providers. The Government relied upon *Smith*'s strong language that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntary turns over to third parties." Petitioner, too, cannot have any subjective expectation of privacy of this information because *Miller* established that one "can assert neither ownership nor possession" of cell-site records and cell phone users generally understand that their phones must communicate with cell towers to make and receive calls. Additionally, cell-phone users cannot have an objectively reasonable expectation of privacy with voluntarily disclosed information to third parties.

In relation to *Jones*, the Government argued that, unlike attaching a GPS device to a vehicle, the Government did not intrude on Petitioner's privacy interests by recording the cell towers used to make his phone calls.¹¹³ The phone companies created these records for their own business purposes.¹¹⁴

In response to Petitioner's claim that the third-party doctrine is not necessarily dispositive when it involves highly sensitive information, the Government worried about "intractable line-drawing problems." Pragmatically, the Government finds it problematic that Petitioner did not provide a framework for defining what is sufficiently sensitive information. Nevertheless, investigators could not even apply this hypothetical standard about sensitivity until they take the first step: accessing the records. 117

The Government argued that this collection of CSLI records failed the property-based analysis since Petitioner "did not create those records and has no right to control their content." Nor could a property interest be grounded in 47 U.S.C. § 222(c)(1) since the statute also permits disclosure "as required by law"—which it is under the Stored Communications Act. 119

```
108. Brief for Respondent, supra note 2, at 28.
```

^{109.} *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

^{110.} Id. at 33–34 (quoting United States v. Miller, 425 U.S. 435, 440 (1976)).

^{111.} Id. at 34.

^{112.} Id. at 37-38.

^{113.} Id. at 54-59.

^{114.} Id. at 59.

^{115.} Id. at 49.

^{116.} *Id.* at 49–50.

^{117.} *Id*.

^{118.} Id. at 68.

^{119.} Id. at 69-70.

The Government also rejected Petitioner's reliance on 47 U.S.C. § 222(c)(1) for calculating an asserted expectation of privacy when the Court previously rejected the suggestion that "the Amendment was intended to incorporate subsequently enacted statutes." ¹²⁰

Moreover, the Government rejected Petitioner's claim about these records "leav[ing] all such data beyond constitutional control, making it possible for the government to collect all Americans' cell-site data for all time" because the Fourth Amendment still protects business records in terms of "arbitrariness, overbreadth, and burdensomeness." Here, the collection of records before and after the unsolved crime was not arbitrary. Since there can be other reasons for Petitioner to be in that area, the several weeks of data can help distinguish which location points are actually relevant.

In response to Petitioner's claims that CSLI will become more precise over time with future technology, the Government suggested that this claim is without merit by providing a hypothetical instance where this would not occur: "[f]or example, device-to-device technology could reduce the need for cell towers, preventing providers from collecting or recording location information." ¹²⁴

Lastly, the Government argued that even if the collection of business records was a search under the Fourth Amendment, it remained constitutionally reasonable¹²⁵ because cases have established that governmental entities can acquire documents via subpoena when Congress authorizes the investigation.¹²⁶ The Government also recognized how certain investigations require subpoenas of this nature because "the very purpose of requesting the information is to ascertain whether probable cause exists." The Government believed the Sixth Circuit correctly held that this warrantless procurement of Petitioner's CSLI records complied with the Fourth Amendment.¹²⁸

^{120.} Id. at 40 (quoting Virginia v. Moore, 553 U.S. 164, 169 n.3 (2008)).

^{121.} Id. at 63.

^{122.} Id. at 64-65.

^{123.} Id. at 65.

^{124.} Id. at 45 (citation omitted).

^{125.} Id. at 70.

^{126.} *Id.* at 72–73 (citing Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946)); *see* Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984).

^{127.} Id. at 75 (quoting United States v. R. Enters, Inc., 498 U.S. 292, 297 (1991)).

^{128.} *Id.* at 90.

V. ANALYSIS

The Supreme Court should reverse the judgment of the Sixth Circuit and hold that accessing CSLI data for an extended period is a "search" under the Fourth Amendment. Thus, the government must show probable cause to obtain a warrant for accessing Petitioner's longer-term CSLI records.

With the need to have a cell phone to be a productive member of society¹²⁹ and the impracticability of living "off the grid," American citizens necessarily have to disclose information to third parties like cellular providers. It does not follow that individuals have to sacrifice any privacy rights or Fourth Amendment protections by owning a cell phone—a device that can enable citizens to be tracked by governmental agencies in unprecedented ways. Chief Justice Roberts has even gone so far as to say that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."130 Therefore, the Court should hold that voluntarily disclosing information to a third party in this manner does not imply that an individual does not have a reasonable expectation of privacy pertaining to that information. The Court should not refer to CSLI data under the façade of being "business records" to downplay an individual's right to privacy like the Court has done in the past with credit card records. 131

The true hardship lies in *Carpenter*'s line-drawing inquiry—at what point does accessing CSLI records become a search under the Fourth Amendment, thereby requiring a governmental entity to show probable cause to obtain a search warrant? Although access to a few location points is not a per se search, ¹³² accessing thousands of

^{129.} See Brief for Petitioner, supra note 1, at 75 ("In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life.") (quoting United States v. Davis, 785 F.3d 498, 525 (11th Cir. 2015) (Rosenbaum, J., concurring)).

^{130.} Riley v. California, 134 S. Ct. 2473, 2484 (2014).

^{131.} United States v. Carpenter, 819 F.3d 880, 895 (6th Cir. 2016) (Stranch, J., concurring) ("In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location.").

^{132.} Petitioner concedes that there is some period of time where the Government can access a person's CSLI free from Fourth Amendment scrutiny. Brief for Petitioner, *supra* note 1, at 53.

location points undoubtedly becomes a search. The existing tests are not suitable to handle this legal question.

Treating CSLI data as business records undermines the comprehensive location data involved and does not help draw territorial lines of what constitutes a search. 133 The reasonableexpectation-of-privacy test created in *Katz* is similarly limited when treating CSLI as mere business records. Even if the Katz inquiry treated cell phones and their CSLI as pieces of property, it is difficult for society to reasonably regard CSLI records as private information when the government and other third parties continuously gain access to what was once perceived as private information. Society does not have to look any further than the WikiLeaks documents about the NSA's capabilities¹³⁴ and by viewing personalized advertisements when scrolling Facebook that are based on past internet search results¹³⁵ to understand that third parties can create comprehensive pictures of us based on our daily habits. Allowing the Government to procure CSLI records without a warrant would essentially allow the government to watch us walk through this world. So, although Americans should have an expectation of privacy with collected information embedded in newer technologies, we do not.

The Sixth Circuit's content/context distinction, too, blurs the line separating searches from non-searches. The test should have to delineate the type of data (CSLI pertaining to incoming/outcoming calls, text messages, emails, apps, etc.) and amount of data that constitutes a search—thus incorporating future changes in technology when CSLI becomes more precise.

Although the Court should undoubtedly recognize that *Carpenter* bears enough resemblance to *Jones* to constitute a search, courts will run into similar issues with future cases where a new technology opens the door for the government to collect data on individuals. Thus, *Carpenter*, as Judge Stranch suggests, calls for the Court to create a new test altogether to handle the situations where "police, using otherwise legal methods, so comprehensively track a person's

^{133.} Id.

^{134.} See Craig Timberg, Elizabeth Dwoskin & Ellen Nakashima, WikiLeaks: The CIA is Using Popular TVs, Smartphones and Cars to Spy on their Owners, WASH. POST, Mar. 7, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying/?utm_term=.f590dcbadbb7.

^{135.} See Noam Scheiber, Facebook's Ad-Targeting Problem, Captured in a Literal Shade of Gray, N.Y. TIMES, Sept. 28, 2017, https://www.nytimes.com/2017/09/28/technology/facebookads.html.

activities that the very comprehensiveness of the tracking is unreasonable for *Fourth Amendment* purposes."¹³⁶ Although precedent is limited by its current landscape, technology continues to grow at an unprecedented rate—changing how society lives and views privacy as a whole. "[O]ur precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances."¹³⁷

Accessing business records should be treated the same way as if a person's location was being physically tracked by a governmental officer. Obtaining few CSLI location points would not be a search under the Fourth Amendment, much like a police officer tailing a suspect's vehicle for a few minutes would not be a search. Katz's subjective element of the test should not be a part of this new test because Americans have widely inconsistent views about what information cell phone providers actually carry and the degree to which we expect the records to be private. The new test should account for how recent technologies are increasingly being incorporated into Americans' daily lives along with how the same technology enables the government to intrude into people's every day affairs without physically following an individual or searching items that are tangibly carried by that person.

A new privacy test that can handle technological advances involving third parties like cellphone service companies and records of information could be as follows:

A person has an expectation of privacy to information data (including information that the person jointly owns) when (1) the expectation is one that society should be prepared to recognize as reasonable and (2) the expectation is similar to the reasonable expectation of privacy regarding similar information data existing before the technology at issue was created.

This test uses the broad term "information data" to account for all types of records and uses the term "jointly owns" because of Chief Justice Roberts' views that cellphone records are a joint venture by the cellphone company and phone owner.¹³⁹ The first element of the

^{136.} Carpenter, 819 F.3d at 896 (quoting United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012)).

^{137.} Id.

^{138.} See United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.").

^{139.} See Amy Howe, Argument Analysis: Drawing a Line on Privacy for Cellphone

test is derived from the *Katz* test but uses the word "should." This is important since it would require a court to make a prescriptive claim about what information ought to be considered private. The second element would force courts to think about comparable information and their respective expectations of privacy before the technology at issue was developed. The Court would compare Petitioner's CSLI data with being tracked by a GPS, albeit a less accurate one, over 127 days. With the freedom to rule about how much the government can intrude into an individual's daily affairs with and without a warrant, the Court can determine the line about how many CSLI location points constitutes a search under the Fourth Amendment, but a bright-line rule is not necessary. The Court can set precedent that CSLI records over 127 days constitutes a search while admitting that they are not deciding the minimum for how many days and location points is always a search. The Court's language should be carefully reasoned since it would guide how the lower courts approach technology and their respective privacy concerns for years to come.

CONCLUSION

Obtaining CSLI records for an extended period of time violates serious privacy concerns when an individual can be comprehensively tracked by their location data. In *Carpenter*, the Court should find that the Fourth Amendment protects this type of information that is disclosed to cellular companies and that requesting these documents is a search under the Fourth Amendment. A governmental entity should have to obtain a search warrant after showing probable cause in order to access these records. A new test that requires the Court to make prescriptive claims about expectations of privacy while comparing newer technologies with older technologies would account for these privacy concerns.