Can police obtain cell-site location information without a warrant? - The crossroads of the Fourth Amendment, privacy, and technology; addressing whether a new test is required to determine the constitutionality of searches pertaining to electronic information

By Jane Lynch and Jared Wagner

While the majority of recent media coverage regarding the Supreme Court has focused on travel bans and allegations of discrimination, another case with even greater possible implications for both constitutional jurisprudence and average Americans is currently before the Court. In *Carpenter v. United States* (S.C. Docket No. 16-402) the Court is being asked to determine whether police investigating a crime must have probable cause and a warrant to obtain cell-site location information (CSLI).

CSLI includes the date, time, and length of each call, the phone numbers involved with each call, and the cell phone tower sites where the call began and ended. Such information is obtained and saved by wireless carriers as part of their ordinary course of business to assist with the process of connecting customers' phones to the strongest available signal. Experts are able to utilize CSLI to determine a phone's approximate location on specific dates and times. The Stored Communications Act (SCA) allows governmental entities to require wireless carriers to disclosure CSLI upon "specific and articulable facts showing that there are **reasonable grounds** to believe that" the information is "relevant and material to an ongoing criminal investigation." 18. U.S.C. § 2703(d).

The outcome of the *Carpenter* case has the potential to establish an entirely new framework for analyzing whether electronic information shared with third-parties is entitled to constitutional protection. This, in turn, could give rise to a new breed of civil rights claims related to the manner in which police obtain and utilize electronic information in general, and CSLI specifically.

A string of armed robberies and a conviction using CSLI obtained upon "reasonable grounds"

Between December 2010 and March 2011, a group of about 20 men were involved in a string of armed robberies committed against Radio Shack and T-Mobile stores in the greater Detroit area. Police arrested a suspect, who confessed and gave the police his cell phone information along with the cell phone numbers of his accomplices. Rather than obtaining a warrant supported by probable cause, the police obtained a court order pursuant to the SCA upon a showing of reasonable grounds, directing the various wireless carriers to provide the CSLI for the accomplices' phone numbers. With respect to Carpenter specifically, the police sought and obtained 127 days of CSLI for his phone number.

Based on the CSLI from Carpenter's phone, the police were able to establish that he was within a half-mile to two miles of each robbery site on the same dates and times that each of the

robberies had occurred. Carpenter filed a motion to suppress the CSLI arguing that it should have been obtained with a warrant supported by probable cause. That motion was denied, and Carpenter was sentenced to 116 years after a jury conviction.

Carpenter's conviction is affirmed based on the third-party doctrine as set forth in prior Supreme Court case law

On appeal, the Sixth Circuit affirmed Carpenter's conviction. *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016). The majority decision held that Carpenter's CSLI was not protected by the Fourth Amendment because it did not involve a physical intrusion on Carpenter's property rights (the wireless carrier created and owned the CSLI) and the information contained in the CSLI was voluntarily provided by Carpenter to a third-party (his wireless carrier). *Carpenter*, 819 F.3d at 885-90. Thus, the Sixth Circuit found that Carpenter did not have any reasonable expectation of privacy in CSLI. *Id.*

In reaching this decision, the majority relied upon several older Supreme Court cases in which a distinction was made between the content of communications (which is entitled to Fourth Amendment protection) and the information necessary to deliver the communications (which is not entitled to Fourth Amendment protection). *Id.* at 886 (citing *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (in which the Supreme Court held that the installation of a device at the telephone company that tracks the numbers dialed from a home phone does not implicate the Fourth Amendment); *Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (in which the Supreme Court held that a search warrant is required to open a letter but the form, weight, and information on the letter, including the recipient's name and address, are not constitutionally protected).

The majority also distinguished as inapplicable several more recent decisions from the Supreme Court involving electronic communications/monitoring. The first case discussed by the majority, *United States v. Jones*, 565 U.S. 400 (2012), held that placing a GPS monitoring device on a vehicle requires a warrant supported by probable cause. *Carpenter*, 819 F.3d at 888-89. That case was distinguished on the grounds that it involved a physical intrusion onto the suspect's property, whereas in this case the police obtained the records from a third-party. *Id.* Additionally, the majority distinguished the precision of a GPS device, which allows police to monitor the whereabouts of a party to within 50 feet, to CSLI, which only allows police to determine the approximate whereabouts of a person within a 120 radial degree half-mile to two mile vector of a cell tower. *Id.* The second case considered and distinguished, *Riley v. California,* 134 S. Ct. 2473 (2014), held that police may not access the contents of a cell phone without a warrant. *Carpenter*, 819 F.3d at 889-90. The Sixth Circuit found that *Riley* "illustrates the core distinction" between police reviewing the contents of communications and/or devices and reviewing data from devices collected by third-parties regarding the device's location. *Id.*

The majority also noted that there was no societal expectation of privacy in CSLI as evidenced by the fact that Congress had enacted a statute expressly allowing the government to obtain such information upon only a showing of reasonable grounds.

A concurring judge suggests the need for a new test to address Fourth Amendment issues related to cellular and internet communications

In a separate concurring opinion, Judge Staunch expressed concern that the previous tests set forth by the Supreme Court and relied upon by the majority regarding privacy concerns were inadequate for dealing with privacy issues related to cellular and internet communications. *Carpenter*, 819 F.3d at 893-97. Judge Staunch's conclusion cited to Justice Sotomayor's statement in her concurring opinion in *Jones* stating that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third-parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third-parties in the course of carrying out mundane tasks." *Id.* at 895 (quoting *Jones*, 132 S.Ct. at 957) (Sotomayor, J., concurring) (citations omitted).

Thus, Judge Staunch concluded that a new test must be developed to determine whether a warrant supported by probable cause is necessary for police to obtain information provided to third-parties as the result of cellular and internet communications. *Carpenter*, 819 F.3d at 895-96. He did not, however, propose the parameters for any such test. *Id.* Moreover, Judge Staunch agreed that Carpenter's conviction should be affirmed regardless of whether the SCA violated the Fourth Amendment by allowing for police to obtain CSLI without a warrant, because the good faith exception to the exclusionary rule would apply since the officers had obtained the disputed information pursuant to a statutory process that had not been previously invalidated. *Id.* at 896.

The Supreme Court accepts certiorari review and conducts oral arguments

Carpenter petitioned the Supreme Court for a writ of certiorari review of the Sixth Circuit's decision. On June 5, 2017, the Court granted the petition and agreed to answer the following question posed by Carpenter: "Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment."

Numerous amicus briefs were filed on both sides of the issue, and oral arguments were held on November 29, 2017. The transcript from these arguments can be found at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf and the audio can be heard at https://www.supremecourt.gov/oral_arguments/audio/2017/16-402. While it is impossible to determine the outcome of a case with any kind of scientific certainty based on the oral arguments, the arguments in this case seem to have provided at least some general insights.

Justices Sotomayor and Kagan appear to be firmly in agreement with Judge Staunch that the third-party doctrine previously adopted by the Court should not be applied to information such as CSLI and a new standard is necessary to address the privacy protections afforded electronic communications by the Fourth Amendment. This stance is not surprising given Justice Sotomayor's statement cited above from her concurring opinion in *Jones*. While not expressly discussing the possible elements for any such new test, the Justices both expressed concern regarding the scope of the search at issue in this case, including the period of time (127 days).

Justice Alito and Chief Justice Roberts appear to support affirming the Sixth Circuit's decision on the basis of the third-party doctrine. While the Sixth Circuit's opinion focused mostly on the Court's decision in *Smith* (which is discussed above), the discussion during oral arguments on the third-party doctrine focused mostly on the case of *United States v. Miller*, 425 U.S. 435 (1976), in which the Supreme Court found that persons do not have privacy interests in bank records reflecting purchases, withdraws, and deposits because such records are compilations of information given to the bank, which is a third-party. As noted by Justice Alito, bank records and the sort of information found not to be entitled to Fourth Amendment protection in *Miller* are arguably much more sensitive and personal than the sort of information the government obtained in this case.

Justices Breyer, Kennedy, Ginsburg, and Gorsuch asked pointed questions of both sides, and their positions are harder to predict. Justice Breyer suggested that the answer to the question is possibly creating an exception to the third-party doctrine rather than scrapping it altogether, such as either limiting the timeframe within which the government would be able to obtain CSLI without a warrant (Carpenter's attorney suggested a 24 hour rule in his arguments) or creating a specific exception to the third-party doctrine for CSLI akin to exceptions previously recognized for medical records. Justice Gorsuch's questions focused on the property interests of customers in CSLI, which, if recognized, could serve as a basis for holding that a warrant is necessary. Finally, Justice Thomas did not ask any questions during the arguments, as is his usual custom, so it is unclear where he stands on this issue.

Practical advice for police officers and municipalities while the Carpenter decision in pending

A decision on the merits will, hopefully, clarify this issue and provide guidance for both police officers and municipalities with regard to the manner in which CSLI and other such information should be obtained during the course of criminal investigations. Until then, however, police will be generally justified in proceeding with obtaining records and information as set forth in the SCA. In addition to the Sixth Circuit, four other Federal Circuit Courts of Appeals have considered this issue and found that obtaining CSLI through the SCA without a warrant does not violate the Fourth Amendment. *United States v. Stimler*, 864 F.3d 253, 263 (3d Cir. 2017) (holding that the transmission of CSLI is involuntary and rejecting the applicability of

the third-party doctrine to it, but still finding that the SCA does not violate the Fourth Amendment because individuals lack a reasonable expectation of privacy in CSLI); *United States v. Graham*, 824 F.3d 421, 425 (4th Cir. 2016) (finding that the third-party doctrine allows police to obtain CSLI without a warrant); *United States v. Davis*, 785 F.3d 498, 513 (11th Cir. 2015); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013).

At this point, the SCA's reasonable grounds provision has not been ruled unconstitutional by either the Supreme Court or a Federal Appellate Court. Thus, the issue of whether CSLI is protected by the Fourth Amendment is, at the very least, unsettled and even if the Supreme Court ultimately finds that a warrant and probable cause are necessary to obtain CSLI, any CSLI obtained by the police pursuant to 18. U.S.C. § 2703(d) prior to any such decision should generally be protected from suppression in a criminal matter under the good faith exception. Indeed, Judge Staunch's concurring opinion in the underlying case is based on that exception, and Justice Alito specifically raised the issue during oral argument asking if Carpenter might not win the war (obtaining a ruling that CSLI requires probable cause and a warrant) but ultimately lose the battle (having his conviction affirmed on the good faith exception). Likewise, the police should also be protected from individual liability under the clearly established prong of the qualified immunity test.

There are, however, still several important issues that should be considered when discussing this issue with police and municipalities. As pointed out by Justice Ginsburg during oral arguments, in the majority of cases police had enough probable cause to obtain CSLI pursuant to a warrant. Indeed, in this case it seems likely that the police could have obtained a warrant for the CSLI from Carpenter's phone based on the specific information given to them by his accomplice. Thus, police should be encouraged to obtain a warrant when they are able to do so. Additionally, the points raised by the Justices during oral arguments seem to suggest that the scope of the information sought is also important to determining whether a constitutional violation has occurred. Therefore, police should also consider limiting the scope of their initial request for information as much as is practical. For example, in this case the police may have considered initially asking for only the CSLI for the dates of the robberies and then seeking additional CSLI, if necessary, based on the knowledge gained from the initial information received.

Municipalities should also consider adopting a formal policy addressing the manner in which CSLI (and other electronic information) are obtained, which directs officers to seek a warrant when available and appropriate. While the police may be individually protected from civil immunity by the lack of clearly established law on this issue, a municipality's liability is arguably not subject to that same standard and the more comprehensive and stringent that a municipality's policy is, whether it be formal or informal, regarding the manner in which CSLI should be obtained by its officers, the better chance that it will not ultimately be held liable if the Supreme Court does find that CSLI is protected by the Fourth Amendment.