New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 05
MONDAY, JULY 10, 2017

OUTSIDE COUNSEL

Expert Analysis

SCOTUS to Decide if Cell Site Location Is Protected by Fourth Amendment

By **Harry Sandick**

And **George LoBiondo**

In recent years, Americans have become more aware of the extent to which the government can seek access to data and records pertaining to their cell phones. In a 2016 study, the Pew Research Center found that 74 percent of Americans say it is "very important" to them that they be in control of who can get information about them. Since 2012, two unanimous decisions by the U.S. Supreme Court have suggested that the justices are sympathetic to these privacy concerns. In both cases, the court relied on the Fourth Amendment to require that law enforcement use a search warrant to obtain data about a person's location or the contents of a cell phone.

On June 5, 2017, the court granted certiorari in *Carpenter v. United States*, No. 16-402, a case that will test whether the justices are again willing to break new ground in the cell phone privacy context. The court will decide whether the government needs a search warrant to obtain historical records of a suspect's cell phone location—or whether it may instead do so under the Stored Communication Act (SCA), which requires the government to show only that there are reasonable grounds to believe that the records are "relevant and material to an ongoing criminal investigation." 18 U.S.C. §2703(d).

Context

Carpenter appears before the court in the wake of two major decisions concerning the balance between privacy and law enforcement in the digital era. In the first of these, *United States v. Jones*, 132 S. Ct. 945 (2012), the court held that the government's use of a GPS device on a suspect's car to monitor his movements constituted a search under the Fourth Amendment. Justice Antonin Scalia's narrow majority opinion reasoned that the government's act of placing the device onto the car was the type of trespass that would have been considered a search when the Fourth Amendment was adopted in 1791.

In separate concurrences, Justices Samuel Alito and Sonia Sotomayor flagged the broader implications of the government's practice. Justice Alito suggested that long-term monitoring "impinges on expectations of privacy," particularly given the ubiquity of cell phones that "now permit wireless carriers to track and record the location of users." Justice Sotomayor cast doubt on the third-party doctrine, which is rooted in "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third

> A ruling for Carpenter may also affect the business practices of cell phone providers and technology companies, which until now have had relatively free reign to use and profit from their users' location data.

HARRY SANDICK *is a partner at Patterson Belknap Webb & Tyler in New York and a member of the firm's white-collar defense and investigations team. He is a former assistant U.S. attorney for the Southern District of New York.* GEORGE LoBIONDO *is an associate in the firm's litigation department in New York.*

parties." This premise, she wrote, "is ill suited to the digital age" and gave the government "a wealth of detail about [one's] familial, political, professional, religious, and sexual associations."

Jones is similar to *Carpenter*: both involve the government learning the location of an individual. However, physical trespass is not needed to collect cell site information. Additionally, the surveillance in *Jones* was not historical, but "real-time"—the officers knew where the car was located, moment-to-moment.

Two years later, in *Riley v. California*, 134 S. Ct. 2473 (2014), the court unanimously held that police generally must obtain a warrant before searching a person's cell phone, even when the phone is seized incident to arrest. Chief Justice John Roberts' analysis began with the observation that smartphones "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." The court rejected the government's attempts to analogize cell phone searches to searches of other records, in view of smartphones' "immense storage capacity" and prevalence in the daily lives of their owners. Traditional exceptions to the warrant requirement, including protection of the arresting officers and the prevention of evidence destruction, did not outweigh the more substantial privacy interests.

'Carpenter v. United States'

Carpenter arose out of an investigation into a series of armed robberies—of cell phone stores, no less—in which the government applied to U.S. magistrate judges for several orders under the SCA. The SCA provides that the government may obtain records and other information (but not "the contents of communications") through a court order upon showing "specific and articulable facts showing that there are reasonable grounds to believe that" the information sought is "relevant and material to an ongoing criminal investigation."

Here, the SCA orders directed cell phone providers to disclose subscriber information and call detail records, including location data, associated with 16 telephone numbers for a period of 152 days. The government used the historical cell site data to prove that Carpenter's cell phone had been in the vicinity of several of the armed robberies when they took place. The government defeated a motion to suppress and then relied on the records in arguing to the jury that Carpenter was "right where the first robbery was at the exact time of the robbery[.]" The jury convicted Carpenter of six robberies, and he was sentenced to more than 116 years' imprisonment.

> Ultimately, Congress must act. It is within the court's domain to articulate when the government's conduct exceeds the protections of the Fourth Amendment, but this is just one of many issues that arise when the SCA—enacted in 1986—is applied to today's technology. For these issues to be addressed, Congress needs to revisit the SCA.

The Sixth Circuit affirmed in a 2-1 decision, holding that the government's collection of the providers' business records did not amount to a search under the Fourth Amendment. Carpenter lacked "any property interest" in the records, and Fourth Amendment protections are applied to the *content* of a communication, not data generated in the course of facilitating those communications. The majority relied on the SCA as a reflection of how society chose to balance the Fourth Amendment concerns at play, deferring to Congress given that rapid technological changes are outside of judges' expertise.

A concurring judge joined only in the outcome, writing that the "sheer quantity of sensitive information procured without a warrant in this case raise[d] Fourth Amendment concerns." Nevertheless, she concluded that even if there were a Fourth Amendment violation, she would affirm because the good faith exception to the exclusionary rule would apply.

Considerations

The Supreme Court granted certiorari on the question "[w]hether 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." To answer this question, the court will have to consider law enforcement's interest in retaining easy access to location information, which has historically been granted less Fourth Amendment protection. At the same time, the justices will be

thinking about the ways that technological advancements have facilitated the erosion of Americans' privacy.

The government has argued that no warrant is required because historical cell site data is often imprecise—in *Carpenter*, the government said that it could only narrow down Carpenter's phone to "within a 3.5 million square-foot to 100 million square-foot area." But the number of cell towers is growing, and cell phone companies are beginning to use "small cells," which makes geolocation more precise. The government now minimizes the importance of this evidence, but the government used this evidence against Carpenter, even referring to it in summation. Also, the government seeks cell site information quite often: One cell phone provider reports receiving over 75,000 requests for location information in a one-year period. The court will have to consider how the volume and scope of these requests affect the Fourth Amendment analysis, if at all.

Both the court's previous rulings and the SCA's text recognize a distinction between the content of a call and other data relating to a phone. If the court now breaks from that paradigm and carves out a privacy exemption to the third-party doctrine, it risks creating an exception that swallows the rule. Could such an exception logically be limited to cell phone records? What about records ordinarily obtained by subpoena, such as landline phone records, or records created by E-ZPass or Uber, which allow the government to retrace a suspect's steps with ease? In the past, the justices have indicated that cell phones are so ubiquitous in modern life that they raise unique privacy concerns. But that notion may already be obsolete as we enter the age of "the Internet of Things," in which not only our cell phones but also household appliances, vehicles, and wearable items connect to the Internet and generate data about our usage. If the court decides to draw a Fourth Amendment line around some of this data, where should the line be drawn?

Several judges also have suggested that the third-party doctrine as it developed in the 20th century should be revisited in the smartphone era. In addition to Justice Sotomayor's comments above, Judge Robin Rosenbaum of the Eleventh Circuit remarked that nowadays "it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis … . And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling."

Implications

Carpenter will have significant implications for cell phone users—that is, most Americans—as well as for law enforcement. The extent of any changes will depend on how broadly the court rules. Will it hold that the type of SCA order at issue in *Carpenter* is per se lawful (or unlawful) under the Fourth Amendment? Or will it seek to apply a limiting principle to the practice, such as a certain level of geographic precision or number of days of records? Will it draw a distinction between live monitoring (*Jones*) and the historical records at issue in *Carpenter*? Law enforcement may have to adjust its investigative practices by making the heightened showing required for a warrant, or by narrowing requests for cell provider data. A ruling for Carpenter may also affect the business practices of cell phone providers and technology companies, which until now have had relatively free reign to use and profit from their users' location data.

Ultimately, Congress must act. It is within the court's domain to articulate when the government's conduct exceeds the protections of the Fourth Amendment, but this is just one of many issues that arise when the SCA—enacted in 1986—is applied to today's technology. For these issues to be addressed, Congress needs to revisit the SCA. Regardless of the outcome here, we agree with those judges and commentators who believe that Congress should amend the SCA to take into account the past three decades of technological development.