December 6, 2017

Supreme Court Searches for Fourth Amendment Line for the Digital Economy

On November 29, 2017, the Supreme Court heard oral argument in *Carpenter v. United States*. The Court's decision could have critical implications for companies operating in the digital economy and their ability to limit government access to data about consumers, particularly so-called non-content data. The oral argument featured justices still in search of a workable limit.

I. The Fourth Amendment's Third-Party Doctrine

The Fourth Amendment generally protects "persons, houses, papers, and effects" in which individuals have a "reasonable expectation of privacy." However, under the "third-party doctrine," developed by the Supreme Court in the 1970s, individuals generally lack a reasonable expectation of privacy in information voluntarily conveyed to third parties. With few exceptions, the government historically has been able to access such data without a warrant. However, due to profound technological advancements, individuals' day-to-day interactions with their digital devices now generate substantially more data about their activities than in the 1970s. Companies retain this data for various purposes, and law enforcement has seized on this retention as a source of evidence in prosecutions. In 2016, for example, Yahoo reported that it received 8,929 civil and criminal government requests for information, and Comcast stated that it received 16,607 criminal subpoenas. Law enforcement has requested data from Internet of Things devices present in many homes, including Amazon's Echo and others.

This trend has heightened concern about the appropriateness of the third-party doctrine in the digital age. In a 2012 concurrence in *United States v. Jones*, Justice Sotomayor bluntly suggested that the doctrine is "ill-suited to the digital age" and "it may be necessary to reconsider" the premise that secrecy is a prerequisite to Fourth Amendment protection.

II. Challenge to the Third-Party Doctrine in *Carpenter v. United States*

In *Carpenter*, the FBI applied for court orders under the Stored Communications Act ("SCA") to obtain the cell site location information ("CSLI") of various suspects, including Timothy Carpenter. Unlike a warrant, an SCA order only requires an application establishing "specific and articulable facts showing that there are reasonable grounds to believe" that the evidence sought is "relevant and material to an ongoing criminal investigation." In response, the cellular companies produced 127 days of CSLI for Carpenter, which was used to establish Carpenter's proximity to a string of robberies. Carpenter's motion to suppress the records on Fourth Amendment grounds was denied, and he was ultimately sentenced to 116 years in prison. On appeal, the majority of a Sixth Circuit panel found that Carpenter lacked a reasonable expectation of privacy in CSLI because it was a business record made by the carrier based on information voluntarily conveyed to it by Carpenter.

III. Concerns from the Justices during Oral Argument

Oral argument reflected a Supreme Court confronting great difficulty in articulating a workable rule that would decide the case without having marked spillover effects into other areas of Fourth Amendment and privacy law. As Justice Breyer remarked, "This is an open box. We know not where to go."

Justice Kennedy expressed doubt that individuals have an expectation of privacy in their cell phone location data. The 81-year-old justice noted that he viewed it as common knowledge that cellular providers collect location data and jokingly remarked that "[i]f I know it, everyone does." Yet the Court clearly struggled with the broader privacy implications of the case, expressing frustration at the difficulty of applying dated case law and statutes to new technologies. Justice Alito remarked that "[n]ew technology is raising very serious privacy concerns," and Justice Sotomayor commented that most Americans "want to avoid Big Brother. They want to avoid the concept that government will be able to see and locate you anywhere you are at any point in time."

Several justices from different ideological perspectives pressed the government on the applicability of the third-party doctrine. Justice Gorsuch, in particular, expressed frustration with the position of the United States, remarking "[I]t seems like your whole argument boils down to if we get it from a third party we're okay, regardless of property interest, regardless of anything else." He summarized the government's argument as "so long as a third party's involved, we can get anything we want." Similarly, Chief Justice Roberts emphasized that CSLI was not a business record "simply created by the company…. It's a joint venture with the individual carrying the phone." Justice Kagan meanwhile pressed for a meaningful reason why data should lose its Fourth Amendment protection merely because it was created with a third party.

IV. Potential Implications of the Court's Decision in *Carpenter*

The case, which will likely be decided in the late spring or early summer of 2018, has significant implications well beyond CSLI. As noted in an *amicus* brief filed by technology companies including Apple, Facebook, Microsoft, and Twitter, devices that are now commonplace require the creation or transmission of vast amounts of metadata. Mobile devices and applications collect location data that is even more precise than CSLI. Wearable devices are generating data regarding consumers' day-to-day lives, including their activity levels and heart rates. Law enforcement is simultaneously trying to use this data in its investigations. In connection with a recent murder case, for example, law enforcement obtained a warrant to access records of the victim's Fitbit exercise tracker, which undermined the defendant's story. In another recent investigation, law enforcement sought data from a suspect's pacemaker to show that the suspect had an elevated heart rate and was not, as he contended, asleep.

Companies collecting data about consumers will want to pay close attention to the outcome of the *Carpenter* case. In particular, *Carpenter* could define the boundaries of what is a reasonable expectation of privacy in the digital realm. While the Fourth Amendment generally applies only to government actors, courts could draw on the Supreme Court's Fourth Amendment analysis when evaluating privacy claims in the non-public realm. *Carpenter* could not only have significant implications for law enforcement, therefore, but also for private companies whose practices around the collection and use of personal information in the United States have been largely guided by what is reasonable and neither unfair nor deceptive. For example, the Court's analysis could influence how companies decide what privacy and security promises to make to their customers in their online privacy policies, and even what data to collect and how to use that data. Among other things, the Court's holding concerning the reach of the government's warrantless access to consumer data could also have implications on data transfers from regions, such as the EU, concerned about the reach of police powers in the United States, with the potential for new or more rigorously enforced barriers to transfer. The *Carpenter* case is an important one to watch.

For more information regarding the Carpenter oral argument or to discuss cybersecurity practices generally, please feel free to contact Rohan Massey, Doug Meal, Heather Egan Sussman, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, Michele Goldman, Kevin Angle, Joe Santiesteban or another member of Ropes & Gray's leading privacy & cybersecurity team.