ROPES & GRAY ALERT

Privacy & Cybersecurity

July 6, 2018

Potential Implications of Supreme Court's Decision in *Carpenter v. United States*

The Supreme Court's term came to a close last week, and it featured several notable cases impacting privacy law. *Microsoft v. United States*, which addressed the government's ability to access data stored overseas, was rendered moot when Congress passed the Clarifying Lawful Overseas Use of Data Act. *Collins v. Virginia*, decided on May 29, limited the so-called "automobile exception" to the Fourth Amendment's search and seizure requirement.

Among the decisions handed down this term with particular significance for clients was the much-anticipated decision in *Carpenter v. United States*, in which the Court held that under the Fourth Amendment, the government must obtain a warrant to access cell-site location information ("CSLI"), the detailed geolocation information collected by cell towers from phones. Even though the decision is directly applicable only to government actors, the case, and particularly its holding on the sensitivity of location data, could have wide-ranging implications for private companies' privacy programs and is also likely to be used by all sides in privacy and data security litigation and enforcement actions.

Carpenter Background

The Supreme Court has generally interpreted the Fourth Amendment to require the government to obtain a warrant based on probable cause where an individual has a reasonable expectation of privacy—for example, if the government seeks to search a person's home or hotel room. The Court has found that an individual has such a reasonable expectation of privacy with their information stored on a mobile device. However, the protection afforded the same data in the hands of a third party, for instance, data stored in the cloud, is less clear. In two cases in the 1970s, the Court held that access to bank statements (*United States v. Miller*) and call records (*Smith v. Maryland*) did not require a warrant. These cases have been interpreted since their inception as formalizing what is referred to as the third-party doctrine, pursuant to which the government generally does not need to obtain a warrant to obtain information that an individual voluntarily disclosed to a third party, even if the information would be otherwise protected by the Fourth Amendment in the individual's hands.

In *Carpenter*, defendant Timothy Carpenter was convicted of criminal charges after police obtained historical CSLI that helped to establish his proximity to a string of robberies. Police did not apply for a warrant when requesting access to the data, which would have required a showing of probable cause to believe that a crime has been or is being committed. Instead, police obtained court orders based only on a reasonable belief that the information was "relevant and material to an ongoing criminal investigation," a lower statutory standard established in the Stored Communications Act. On appeal, the Court of Appeals for the Sixth Circuit concluded that Carpenter lacked a reasonable expectation of privacy in the CSLI because it was a business record made by the service providers based on information voluntarily conveyed to them by Carpenter.

Carpenter Decision

In a decision authored by Chief Justice Roberts and joined by four other justices, the Supreme Court reversed, ruling that an individual's reasonable expectation of privacy in his or her location is violated by access to seven or more days of historical CSLI (seven days was the amount of historical CSLI requested from Sprint Corporation in response to one of the court orders at issue; separately, 152 days of data was requested from MetroPCS). The Court concluded that access to such CSLI impermissibly enables police, at minimal expense, to conduct "near perfect"

surveillance of an individual's physical movements, "as if it had attached an ankle monitor to the phone's user" "not for a short period but for years and years." According to the Court, this access amounted to an invasion of "the privacies of life" with the potential to reveal "familial, political, professional, religious, and sexual associations."

The Court further explained that its holdings on the third-party doctrine considered not only the voluntary conveyance of information, but also the nature of the information at issue. The Court found that CSLI is "qualitatively different" from the bank or phone records at issue in prior cases, which revealed little in the way of identifying information or were commercial transactions. The Court also found that, unlike bank and call records, individuals do not in practice "voluntarily" give their CSLI to third-party service providers because carrying a phone that regularly generates CSLI is "indispensable to participation in modern society."

The Court stressed that its ruling was a narrow one. The opinion explicitly stated it was not addressing police access to other types of records, including smaller amounts of historical CSLI, real-time CSLI, "tower dumps" (a download of information on all the devices that connected to a cell site during a particular interval), conventional surveillance techniques and tools such as security cameras, and other business records that might incidentally reveal location information. The Court explained that it planned to "tread carefully in such cases" so as not to "embarrass the future."

Potential Implications

Although the ruling directly affects only government actors, private companies should also take note of its impact. As an initial matter, for companies collecting CSLI, the case provides a clear basis to push back against any request made by law enforcement for CSLI without a warrant. While the Court stressed the narrowness of its holding, the Court also explained that the litmus test is whether the "suspect has a legitimate privacy interest in [the] records." That breadth, along with the Court's concern for revealing "familial, political, professional, religious, and sexual associations" may also support arguments for extending protections to other forms of location data, and possibly to other forms of potentially sensitive data as well. Companies collecting data through the Internet of Things (IoT), for example, may have a basis to resist warrantless requests, given the invasion of an individual's privacy interest in the home, and the potentially sensitive nature of the data collected.

Companies may also want to consider how their interactions with customers could impact the customer's "reasonable expectation of privacy," and consequently, their ability to push back against a warrantless request for information. Promises made regarding the privacy of the data at issue could impact such expectations, as could a customer's agreement, typically in terms of use, to disclosure of the information in question. Consequently, if a company wishes to protect closely its customers' data, it should carefully draft its privacy policy, terms of use, and other public-facing statements, including statements describing how the company responds to government access requests. Before companies revise any terms, however, they should carefully weigh the potential benefit of such revisions against any potential for increased liability exposure.

Privacy and data security plaintiffs' lawyers have stated that they plan to use the Court's ruling to support arguments that location information has intrinsic value or is uniquely sensitive. However, the persuasive value of this opinion is limited because it occurs in the Fourth Amendment context, rather than in the contexts in which those statutes and common law rights are commonly litigated, and the Court on several occasions explicitly cabined its holding. Plaintiffs' lawyers or regulators may nevertheless try to analogize the Court's holding to the treatment of CLSI, or data other than CSLI, in settings beyond the Fourth Amendment's governmental "search and seizure" scope. Companies collecting CSLI or similar information may, accordingly, wish to evaluate their practices for collecting and processing such information, and to review the privacy and cybersecurity protections they have in place.

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