wiley

ALERT

Carpenter v. United States: The Supreme Court's Recent Decision Will Have Widespread Implications for the Collection of Digital Information by Law Enforcement

June 25, 2018

On June 22, 2018, in a major decision on data privacy, the U.S. Supreme Court held that the government must obtain a warrant when seeking historical cell tower records providing a detailed and comprehensive history of a user's movements. The Supreme Court's holding has widespread implications for all companies that collect user data and may require companies to re-evaluate how they comply with legal process in certain instances.

Overview of *Carpenter v. United States*

Factual Overview: In 2011, the Federal Bureau of Investigation (FBI) suspected Mr. Carpenter of robbing a string of Radio Shacks and T-Mobile stores in Detroit, Michigan. The FBI issued an order under 18 U.S.C. § 2703(d) to both MetroPCS and Sprint – Mr. Carpenter's wireless carriers – seeking cell site information for Mr. Carpenter's cell phone for the four-month period in which the robberies occurred. An order pursuant to 18 U.S.C. § 2703(d), often referred to as a 2703 (d) Order, allows the government to compel disclosure of certain "non-content" information when the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation."

The FBI ultimately used the cell-site information at trial to prove that Mr. Carpenter was near each store at the time of the alleged robberies. Before his conviction, Mr. Carpenter moved to suppress the

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Vesna K. Harasic-Yaksic
Partner
202.719.4506
vharasic-yaksic@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Telecom, Media & Technology

cell-site data, arguing that the government's seizure of these records violated the Fourth Amendment because it was not obtained pursuant to a warrant supported by probable cause. The Sixth Circuit affirmed the conviction and the Supreme Court granted certiorari.

Legal Analysis: The Supreme Court reversed the Sixth Circuit's decision, concluding that obtaining cell-site location information (CSLI) requires a warrant supported by probable cause. In its opinion, the Court analyzed cases establishing the third-party doctrine, which had previously held that a person has no legitimate expectation of privacy in information that he or she voluntarily discloses to third parties.

Noting that CSLI "does not fit neatly under [these] existing precedents[,]" the Court ultimately declined to extend the third-party doctrine to CSLI. According to Chief Justice Roberts, CSLI is akin to GPS information in that it provides an extraordinary amount of personal information: it "provides an intimate window into a person's life revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.'" Moreover, because cellphones are such a necessary part of daily life, it cannot be said that CSLI is "truly shared as one normally understands the term." Therefore, "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party [.]"

Implications of *Carpenter v. United States*

The Supreme Court's decision in *Carpenter* limits application of the third-party doctrine in light of the ability of modern technology to collect data. The opinion not only acknowledges that transmission of data in the digital age reveals a wealth of information about an individual's personal life, but also that participation in technologies is a necessity of modern life. In recognizing these principles, the opinion makes clear that the government can no longer argue that individuals using digital technology somehow assume the risk of warrantless government action.

Carpenter should not be interpreted in isolation. Rather, *Carpenter* is the third recent case where the Court has expressed its willingness to expand Fourth Amendment principles and adopt a flexible approach to protecting the privacy of digital information. In *United States v. Jones*, the Supreme Court limited the government's ability to use a GPS device to track an individual's movements. Additionally, in *Riley v. California*, the Supreme Court declined to extend the search-incident-to-arrest doctrine to cell phone searches, stating that "the storage capacity of [a] cell phone" allows it to "collect[] in one place many distinct types of information… that reveal more in combination than any isolated record." Collectively, these cases signify that the Court believes that the Fourth Amendment provides a strong check on law enforcement when it comes to the collection of digital information.

As courts and law enforcement work to understand the limits of *Carpenter*, companies that collect user data should consider the following:

- Companies will still enjoy broad protections when they respond to law enforcement requests in good faith.

- Companies may need to review how they respond to subpoenas and 2703(d) Orders in certain cases—particularly requests for location information.
- *Carpenter* expressly held that the emergency exception to the Fourth Amendment's warrant requirement still applies to location information. Companies may continue to process these requests under their existing policies.
- The scope of the Court's holding beyond the facts of the case (a 2703(d) Order seeking location information during a four-month period) is unclear. However, the Court's limitation of the third-party doctrine and expanded interpretation of a user's privacy interests suggests a broad ruling. Companies will have to consider whether the Court's ruling has extended Fourth Amendment protections (and a warrant requirement) to other classes of collected data.