Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# High Court Gets Ready To Weigh Privacy Vs. Public Safety

By **Bob Anderson**
November 1, 2017, 5:39 PM EDT


Bob Anderson

The gunmen who stole mobile phones from a series of Radio Shacks in Detroit probably weren't strict constitutionalists.

But the facts surrounding their arrest and conviction could have a serious impact on the extent of privacy protection under the Fourth Amendment, and how police use modern surveillance techniques to gather evidence in criminal investigations.

The case in question, Carpenter v. United States, will soon be before the U.S. Supreme Court, which will weigh personal privacy against public safety. Specifically, the court will decide how much latitude law enforcement has in conducting warrantless searches for cell tower data and similar types of metadata.

The Fourth Amendment requires law enforcement to show probable cause and obtain a warrant to search and seize property and effects.

But for years, law enforcement has routinely conducted warrantless searches to gather information on metadata, which is essentially “data about data.” A familiar example of metadata is the call list on a cellphone bill, which identifies the day, time, number dialed, location, and length of each call.

Cell tower sites gather similar noncontent metadata, and law enforcement routinely uses it to track the activity and movement of criminal suspects. Courts have generally allowed warrantless search of such data because it is simply a record of communications, not the contents of the calls.

Police were able to use cell tower data to prove that the Carpenter gang was staking out and robbing cellphone stores. Carpenter's defense team challenged the right of police to collect the cell tower data without proving probable cause and securing a warrant.

Carpenter v. United States could dramatically affect the future of surveillance, potentially requiring law enforcement to secure a warrant each time it seeks metadata about cellphone calls, text messages, emails, credit card activity and similar records.

The Supreme Court will be weighing the balance between a citizen's privacy rights and the ability of law enforcement to quickly track suspects in crimes ranging from crude holdups, like the Carpenter case, to

more urgent circumstances, such as trying to locate a kidnapper or a terrorist.

**The Case**

Police in Detroit were puzzled by a string of robberies in which a group of armed suspects would rush into Radio Shack and T-Mobile stores, order customers and employees into the back room, and clean out the cellphone inventory. The investigation expanded following similar robberies in the Detroit suburbs and Warren, Ohio.

Police arrested four suspects in April 2011, and one of the suspects confessed to the crimes, identified his co-conspirators, and their cellphone numbers.

Half-brothers Timothy Carpenter and Timothy Sanders were identified by police as the ring leaders. They were accused of planning the robberies, supplying the guns, acting as lookouts while their team robbed the stores, and driving the getaway cars.

To help build their case, police and the FBI obtained data from cell tower sites near the stores, trying to place the suspects in the area on the days and times of the robberies. Authorities obtained court orders for those records under the Stored Communications Act, which requires a reasonable belief of criminal activity to request the data. That threshold is much lower than the Fourth Amendment, in which authorities need to prove probable cause and obtain a warrant.

As a result, the FBI said it was able to place Carpenter and Sanders within one-half mile to two miles on the day and time of some of the robberies. Carpenter was sentenced to 116 years in prison, and Sanders, 14 years.

**The Appeal**

Appealing their convictions, Carpenter and Sanders, with help from the American Civil Liberties Union, sought to suppress use of the cell tower data. They argued that law enforcement was obligated under the Fourth Amendment to cite probable cause and obtain a warrant to collect the cell tower data. They also contended that the FBI's request for 127 days of Carpenter's cellphone data and 88 days of data from Sanders was such a lengthy time period that it violated their reasonable expectations of privacy, again triggering the need for authorities to obtain a warrant.

A federal appeals court upheld the conviction, stating that the cell tower site data should not be considered private property under the Fourth Amendment, and therefore, authorities did not need to show probable cause or obtain a warrant.

“The cell site data — like mailing addresses, phone numbers, and IP addresses — are information that facilitate personal communications, rather than part of the content of those communications themselves,” the appeals court wrote. “The government's collection of business records containing these data therefore is not a search.”

But the appeals court also issued this additional observation: “The runaway pace of technological development [means] we have more work to do to determine the best methods for assessing the application of the Fourth Amendment in the context of new technology.”

**The Impact**

Perhaps the “runaway pace of technological development” and its impact on public personal privacy versus public safety is the reason the Supreme Court decided to take up Carpenter v. United States.

Modern surveillance is built on law enforcement's ability to quickly obtain and assess metadata, searching for communication time stamps, locations, and patterns to help solve crimes. Should the Supreme Court rule to restrict those searches because they violate the Fourth Amendment, then police investigations would be slowed by the need to show probable cause and obtain a warrant.

Law enforcement agencies across the country conduct thousands of metadata investigations daily, looking for patterns in cellphone calls, texts, emails and social media. Many of those searches turn out to be fishing expeditions. But sometimes they help authorities uncover criminal activity, including terrorist threats. Law enforcement worries that those investigations would slow to a crawl should it be necessary to go to court and get a warrant for each metadata search.

On the flip side, personal privacy issues are also at stake, considering the rapid development of new forms of communication, and how there is a permanent record of each phone call, email, text, and social media post we make.

“The number and variety of organizations and experts filing represent the widespread recognition that your cellphone's location history is your own business, and the government needs to have a good reason to get its hands on it,” according to a statement from Nathan Freed Wessler, a lawyer for the ACLU.

Meanwhile, large technology companies, including Apple Inc., Facebook Inc. and Google Inc., have filed an amicus brief in Carpenter v. United States asking the Supreme Court to “refine the application of certain Fourth Amendment doctrines to ensure that the law realistically engages with internet-based technologies and with people's expectations of privacy in their digital data.”

Given the mounds of data we generate through use of our mobile devices, computers, credit cards, bank transactions and other activities, the Supreme Court has an opportunity to determine how broadly the Fourth Amendment applies to 21st century communication.

---

*Bob Anderson is a managing director in the Washington, D.C., office of Navigant Consulting Inc. and leader of the firm's information security practice.*