Police Prosecutor Update

Issue No. 311
June 2018
Special Edition

SEARCH AND SEIZURE
CELL SITE LOCATION INFORMATION DATA

On June 22, 2018, the United States Supreme Court issued its decision in Carpenter v. U.S, ___ U.S. ___ , 2018 U.S. LEXIS 3844. After arresting four men suspected of robbing Radio Shack and T-Mobile stores, police narrowed their investigation on a group that had robbed nine different stores in Michigan and Ohio. Carpenter was the leader of this group, and police had obtained his cellular telephone number and the numbers of some of his confederates. Based upon that information, prosecutors applied for court orders to obtain the cell phone location records for Carpenter and others through the Stored Communications Act. Similar to a prosecutor's subpoena duces tecum, such an order may be granted when "specific and articulable facts show . . . that there are grounds to believe" that the records "are relevant and material to an ongoing criminal investigation." The order was granted.

Cell phones interact with "cell sites," which both receive signals from and broadcast a signal to the cell phone. "Each time the phone connects to a cell-site, it generates a time-stamped record known as cell-site location information (CSLI)," which wireless carriers store for a variety of business purposes. "Modern cell phones generate increasingly vast amounts of increasingly precise CSLI."

After Carpenter lost his motion to suppress in the trial court, seven of his confederates identified him as the leader of the criminal enterprise, and expert testimony placed Carpenter's phone near four of the charged robberies. Carpenter was convicted of the robberies. On appeal, the Sixth Circuit affirmed the denial of Carpenter's motion to suppress. "Given that cell phone users voluntarily convey cell-site data to their carriers as 'a means of establishing communication,' the court concluded that the resulting business records are not entitled to Fourth Amendment protection."

The Supreme Court recognizes constitutional protection for places and things in which an individual has a "legitimate expectation of privacy." Where a person has voluntarily turned over information to third parties, there is no legitimate expectation of privacy. Thus, banking records and numbers dialed from a landline telephone were not protected by Fourth Amendment. Cell phones, however, are different. While the individual continuously reveals the location of his cell phone (unless he turns it off) to his wireless provider, "cell phone location information is detailed, encyclopedic, and effortlessly compiled." Finding the cell-phone "almost a 'feature of human anatomy'" (the court cited a statistic that 12% of smart phone owners admitted using their phones in the shower), the court found that CSLI provides police with access to "a category of information otherwise unknowable." "It is . . . a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."

A warrant based upon probable cause is now required to obtain historic CSLI. The Court left unanswered whether a warrant is required for real-time CSLI "tower dumps", or "other business records

This is a publication of the Prosecutor's Office which will cover various topics of interest to law enforcement officers. Please direct any questions or suggestions you may have for future issues to the Prosecutor's Office.

that might incidentally reveal location information." Exigent circumstances may also justify the warrantless acquisition of CSLI. The prudent law enforcement officer from here on out should seek a search warrant, unless exigent circumstances exist, for records in the possession of third parties that could implicate the person generating those records in criminal activity.