Prosecuting Attorneys' Council of Georgia

State Prosecution Support Division

fyi

JUNE 22, 2018

FYI: CARPENTER v. UNITED STATES

The United States Supreme Court Rules that the Acquisition of a Defendant's Cell-Site Records is a Fourth Amendment Search

In *Carpenter v. United States*, No. 16-402 (June 22, 2018), the FBI identified the cell phones of several suspects in a string of robberies. Each time a cell phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. The Stored Communications Act permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." Federal prosecutors applied for, and were granted court orders under the Act to obtain CSLI from Carpenter's wireless carriers. Specifically, the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days – an average of 101 points per day.

Carpenter moved to suppress the data, arguing that obtaining his records from his wireless carrier violated the Fourth Amendment because it was done without a search warrant supported by probable cause. The trial court denied the motion. The federal appeals court affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information because he had shared that information with his wireless carriers. In a 5-4 decision, the Supreme Court reversed.

The Government contended that the third-party doctrine governs this case because cell-site records are "business records" created and maintained by wireless carriers. The Court disagreed. The Court stated that the third-party doctrine stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with others. But, the doctrine's foundation did not rely solely on the act of sharing, and mechanically applying the doctrine in this case would fail to appreciate the lack of comparable limitations on the revealing nature of CSLI. Also, CSLI is not truly "shared" because 1) cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society; and 2) cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond just powering up. Thus, given the unique nature of CSLI, the Court declined to extend the third-party doctrine to cover them.

1590 Adamson Parkway, 4th Floor • Morrow, Georgia 30260 • (770) 282-6300 • Fax: (770) 282-6368

Rather, the Court found, tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *U.S. v. Jones*, 565 U.S. 400 (2012). In fact, the Court stated, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers. Furthermore, the Court added, any rule it adopts must take into account the more sophisticated systems that are already in use or in development. And, the Court noted, the accuracy of CSLI is rapidly approaching GPS-level precision.

Thus, the Court concluded, given the unique nature of CSLI, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. "[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search." Therefore, "we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records."

But here, the Government did not obtain such a warrant before obtaining the CSLI. Instead, the records were obtained under the Stored Communications Act which requires a showing that falls well short of the probable cause needed for a warrant. Thus, the Court further held, an order issued under the Act is not a permissible mechanism for accessing historical cell-site records, and the trial court erred in denying Carpenter's motion to suppress.

In so holding, the Court stated that not all orders compelling the production of documents will require a showing of probable cause. A warrant is required only in the "rare case" in which the subject has a legitimate privacy interest in records held by a third party. Moreover, the Court emphasized, its decision in this case "is a narrow one." The Court expressed no view on matters not before it: real-time CSLI, "tower dumps," or collection techniques involving foreign affairs or national security. Finally, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records. For example, exigent circumstances which would include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or to prevent the imminent destruction of evidence.

1590 Adamson Parkway, 4th Floor • Morrow, Georgia 30260 • (770) 282-6300 • Fax: (770) 282-6368