LOS ANGELES COUNTY DISTRICT ATTORNEY'S OFFICE

ONE MINUTE BRIEF

JACKIE LACEY
DISTRICT ATTORNEY

NUMBER: 2018-11 **DATE: 06-22-18** **BY: Devallis Rutledge** **TOPIC: Cell-site Surveillance**

ISSUE: Does law enforcement access to historical data from cell-phone sites constitute a Fourth Amendment "search," requiring a warrant or recognized exception?

Whether in use or not, cell phones continually scan ("ping") for the nearest cell tower, and as the phone moves with its user, connectivity is relayed from tower to tower. A record of the dates, times and locations of cell-phone pinging allows law enforcement officers to derive the past movements of individuals, thereby placing them in the vicinity of a crime, or not. Records produced by this constant tracking process are sometimes called "cell-site location information," or CSLI. Are such records subject to Fourth Amendment protection, requiring a warrant or recognized exception for investigative access?

● Timothy Ivory Carpenter was part of a criminal gang that robbed nine stores in Michigan and Ohio. The FBI learned Carpenter's name and cell-phone number from an accomplice, obtained his CSLI for the dates of the robberies, and established his location in the vicinity of six of the robberies. After Carpenter's motion to suppress the evidence resulting from the warrantless access to his historical CSLI was denied, he was convicted, and he appealed.

Lower courts held that suppression was not required, on the grounds that Carpenter voluntarily revealed his cell activity to the service provider and therefore lost any legitimate expectation of privacy, and that agents had obtained a court order for the CSLI under the Stored Communications Act, 18 USC § 2703(d). On *certiorari,* the US Supreme Court has now reversed (5-4):

"[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." Carpenter v. US (2018) 585 US ___ , Slip opn. at 11.

The court also held that the court order, not satisfying the requirements of sworn probable cause necessary for a search warrant, could not be relied on to justify the search: *"Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant." Id.,* Slip opn. at 19.

● Calling its decision *"a narrow one"* (Slip opn. at 17), the court said that its ruling **did not affect** real-time "tower dumps" (which reveal information on **all** the devices pinging on a certain site at a particular time), nor security-camera evidence. The court also reaffirmed that **exceptions** to the warrant requirement could permit access, suggesting warrantless access could be justified where information was needed immediately in such cases as bomb threats, active-shooter situations, child abductions, pursuit of dangerous suspects, preventing imminent danger, or preventing the imminent destruction of evidence. Slip opn. at 21-22.

● Law enforcement officers in California already routinely apply for search warrants to obtain CSLI, as generally required by the California Electronic Communications Privacy Act. PC §§ 1546-1546.4. See 1MB *Extra* 2016-X1.

● In a series of cases, the Supreme Court has ruled that other kinds of businesses may voluntarily share with law enforcement officers their business records and other information about customers, subscribers, depositors, *etc.*, on the ground that an individual may no longer maintain a legitimate expectation of privacy after voluntarily disclosing information to a third party, knowing that the third party may reveal that information to police. *US v. Miller* (1976) 425 US 435, 443 (bank records); *Smith v. Maryland* (1979) 442 US 735, 741 (phone company call records); *US v. Jacobsen* (1984) 466 US 109, 121 (open FedEx package). **These authorities remain valid:** *"We do not disturb the application of Smith and Miller…."* Slip opn. at 18.

<u>BOTTOM LINE</u>: Accessing historical cell-site location information is a Fourth Amendment "search," requiring a warrant or recognized exception.