Conducting Surveillance and Collecting Location Data in a Post-Carpenter World, Part II

Posted on Oct. 5, 2020, 3:27 pm by Shea Denning

This post is the second in a series examining the impact of *Carpenter v. United States*, 585 U.S. ___, 138 S.Ct 2206 (2018) on electronic surveillance and the obtaining of location and other types of information from third parties. The first post in this series summarized post-*Carpenter* decisions relating to surveillance by pole camera and tower dumps. This post examines post-*Carpenter* rulings on the obtaining of real-time surveillance information through satellite-based Global Positioning System data (GPS) or cell site location information (CSLI). The last post in this series will examine the use of cell site simulators and the obtaining of other information about a person's on-line activities or accounts from third parties.

[Author's Note: If you have been paying close attention, you will know that I initially planned to cover all five categories in two posts. There was simply too much material. I will address cell site simulators and other third party data in a subsequent post.]

Real-time surveillance. The information obtained by the government in Carpenter was ***historical*** CSLI. Carpenter was not being surveilled at the time the robberies occurred. Instead, after he was identified as a suspect, the government obtained CSLI from the companies that provided service to his mobile phone. Those records showed that Carpenter was right "where the . . . robbery was at the exact time of the robbery." 585 U.S. at ____; 138 S.Ct. at 2213.

In many cases, however, the government may wish to ***proactively*** monitor a known suspect by having a wireless communications provider gather CSLI information or GPS coordinates from the suspects' phone. The *Carpenter* majority specifically stated that it was not expressing a view on the collection of real-time CSLI or GPS, so post-*Carpenter* courts have been sorting out whether and how *Carpenter* and the Fourth Amendment cases upon which it relied apply to real-time surveillance.

Real time CSLI or GPS before *Carpenter*. Even before *Carpenter*, some courts considered the collection of real-time location information from a person's cell phone to be a Fourth Amendment search. *See, e.g.*, *Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014) (holding that the use of the defendant's CSLI to track him in real time was a Fourth Amendment search); *see also United States v. Espudo*, 954

F. Supp. 2d 1029 (S.D. Cal. 2013) (finding that the majority of federal courts examining the requirement for acquiring real-term cell site location data required a showing of probable cause). Others did not. *See, e.g., United States v. Skinner*, 690 F.3d 772 (2012) (concluding that the defendant had no reasonable expectation of privacy in the data emanating from his phone that the government used to determine its real-time location).

The collection of real-time data differs from the acquisition of historical data in ways that may be significant to the constitutional analysis. Real-time data enables law enforcement officers to locate a person in the first instance so that the person then may be surveilled. In that respect, it is significantly more intrusive than traditional surveillance, which requires that a person be located as a precondition to tracking the person's movements. On the other hand, real-time location information may be sought for a shorter duration of time than historical CSLI. When, for example, real-time information is used to locate a suspect for purposes of making an arrest, it may cover only a few hours of time.

Another distinction between the government's acquisition of historical CSLI and real-time CSLI is that the former is a record maintained in the wireless provider's ordinary course of business while, in some instances, the latter is not. A communications provider may identify the real-time location of a phone by "pinging" it (sending a request to the phone's command center) at the request of law enforcement. *See Commonweath v. Pacheco*, 227 A.3d 358, 363 (Pa. Super. 2020), *appeal granted in part,* 2020 WL 4332936 (Pa. July 28, 2020). The signal activates the phone's location subsystem to determine its location. *Id*. If the phone has GPS functionality (as most phones do) and is turned on, the phone company can then identify the latitude and longitude coordinates of the phone as identified by satellite. *See United States v. Riley*, 858 F.3d 1012, 1014 n.1 (6th Cir. 2017) (explaining this methodology); *see also Commonwealth v. Almonor*, 120 N.E.3d 1183, 1193 n.12 (Mass. 2019) (noting that "today, virtually all cell phones contain a GPS receiver, thereby giving police the capability to ping the cell phones of hundreds of millions of people"). If GPS data cannot be obtained, the phone's location is identified by the closest cell tower. *Pacheco*, 227 A.2d at 363. The cell phone transmits its location (which generally is accurate within about 30 yards) back to the wireless provider, which then sends the information to law enforcement. *Id.*

When a phone company tracks down a phone by intentionally activating its GPS system, it arguably is not collecting information for business purposes at all, but instead is acting as the agent of law enforcement. *See Almonor*, 120 N.E.3d at 1193 (stating that the data obtained when a cell phone is pinged would not otherwise be collected and retained by the service provider). Thus, the third-party doctrine, which hinges in part on a person's voluntary sharing of data with a third party for its business use, may have no application to this sort of data collection. *See, e.g.*, *United States v. Caraballo*, 963 F. Supp. 2d 341, 360 (D. Vt. 2013), *aff'd*, 831 F.3d 95 (2d Cir. 2016) (stating that "the instant case is

distinguishable from *Smith* [*v. Maryland*] and [*United States v.*] *Miller* as pinging simply is not part and parcel of the provision of cellular phone service"). If that is so, then the act of obtaining information about a person's whereabouts (which the person has not elected to reveal to the public) may be a Fourth Amendment search.

***Commonwealth v. Pacheco*, 227 A.3d 358 (Pa. Super. 2020), *appeal granted in part,* 2020 WL 4332936 (Pa. July 28, 2020).** In *Pacheco*, the Superior Court of Pennsylvania determined that when "prosecutors sought and obtained real-time information about Pacheco's location by pinging his cell phone, they conducted a 'search' under the federal and state constitutions." *Id.* at 370.

Pacheco was investigated by federal and state agents for his involvement in a heroin-trafficking operation. At various times throughout the nearly year-long investigation, prosecutors applied for and obtained orders that authorized Pacheco's cell phone company to ping his phone at times directed by law enforcement. These signals gave investigators real-time location information. Based on that information, investigators identified multiple occasions when Pacheco traveled to Georgia and New York. They learned that on each trip Pacheco obtained a car battery containing three kilograms of heroin in Georgia, returned briefly to Pennsylvania and then transported the heroin to New York.

Pacheco was charged with numerous drug crimes. He moved to suppress the real-time CSLI evidence. The trial court denied his motion. Pacheco was convicted and appealed, alleging that, among other errors, the trial court erred in denying his motion to suppress.

The Pennsylvania appellate court found no "meaningful distinction between the privacy issues related to historical and real-time CSLI" and concluded that *Carpenter*'s rationale applied to real-time CSLI tracking. The court held that a person maintains a legitimate expectation of privacy in his physical movements as captured through real-time CSLI and that when the government had Pacheco's wireless provider "ping" his cell phone, it conducted a Fourth Amendment search. The court went on to conclude that the court orders that prosecutors secured to obtain this information were in fact warrants under the Fourth Amendment. They were based on probable cause, were issued by a neutral and detached judicial official, identified the person and the criminal offenses, and described the place to be searched and the items to be seized.

***Sims v. State*, 569 S.W.3d 634 (Tex. Crim. App. 2019).** The Court of Criminal Appeals of Texas concluded in *Sims* that while *Carpenter*'s reasoning applied to real-time CSLI, the defendant did not have an expectation of privacy in his physical location or movements as reflected in less than three hours of real-time CSLI records access by law enforcement by pinging his phone fewer than five times.

Sims was charged with murder for shooting and killing his grandmother. He fled in his grandmother's car. Law enforcement officers used real-time CSLI to track him to a motel in Oklahoma, where he was arrested. Sims moved to suppress evidence gathered based on the real-time CSLI. The trial court denied the motion. Sims was convicted and appealed.

The appellate court considered the Court's reasoning in *Carpenter* to apply to both historical CSLI and real-time location information. It characterized the analysis of whether a particular government action constitutes a search or seizure as turning on whether the government seized "'enough'" information such that it violated a legitimate expectation of privacy. *Sims*, 569 S.W.3d at 646. Noting that *Carpenter* held that the government conducted a search when it accessed at least seven days of Carpenter's CSLI, the *Sims* court stated that whether a person has a recognized expectation of privacy in real-time CSLI records must be decided on a case-by-case basis. In Sims' case, the court determined that Sims "did not have a legitimate expectation of privacy in his physical movements or location as reflected in the less than three hours of real-time CSLI records access by police by pinging his phone less than five times." *Id.*

GPS Monitoring. *Carpenter* relied in part on the view expressed by five concurring justices in *United States v. Jones*, 565 U.S. 400 (2012), that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones* was, however, decided on other grounds; the majority determined that the installation of a GPS tracker on the suspect's car was search because it involved the obtaining of information through a physical trespass. *Id*. at 404-05. And the Supreme Court earlier held in *United States v. Knotts*, 460 U.S. 276 (1983), that the government did not conduct a Fourth Amendment search when it placed a beeper in a container so as to monitor the location of the car carrying the container, which traveled on public roadways to the defendant's cabin. No search occurred, the *Knotts* Court reasoned, because by traveling over the public streets, the car's driver voluntarily conveyed his location to anyone who wanted to look. *Id*. at 281-282. While the tension between *Carpenter*'s acknowledgment that individuals have a reasonable expectation of privacy "in the whole of their physical movements" and *Knotts*' view of what a person voluntarily exposes to the public is clear – the resolution is less so. Thus, the question of whether GPS monitoring of a suspect without committing a physical trespass constitutes a Fourth Amendment search remains open.

***United States v. Howard*, 426 F. Supp. 3d 1247 (M.D. Ala. 2019).** The federal district court for the Middle District of Alabama considered whether "the Government gets one free day to electronically track a borrowed truck with a GPS tracking device without a warrant," determining on the facts at issue that it did.
In *Howard*, a confidential informant agreed to allow investigators to install a GPS tracker on her truck, which she loaned to the defendant for a trip to pick up methamphetamine. The GPS device transmitted the truck's location every five

seconds while the truck was in motion. Investigators monitored the truck's movements for nineteen hours as it traveled from Dothan, Alabama to Phenix City, Alabama and back. Howard was stopped as he returned to Dothan and investigators found methamphetamine in the truck. At his trial on federal criminal charges, Howard moved to suppress the evidence obtained as a result of the GPS monitoring of the borrowed truck.

The trial court denied the motion, determining that Howard had no reasonable expectation of privacy pursuant to the principles set forth in *Knotts*. First, the court noted that there was no trespass, as the borrowed truck was equipped with owner-approved GPS tracking. Second, the surveillance was not for an extended period of time. Howard was monitored during a single trip lasting less than 24 hours over a distance of approximately 200 miles. Third, the court distinguished GPS vehicle monitoring from CSLI, describing the latter as more intrusive both because it is retrospective and because cell phones, unlike vehicles, track nearly exactly the movements of their owners. Finally, the *Howard* court said its holding was grounded in stare decisis: While *Carpenter* may signal the Court's willingness to revisit *Knotts*, the high court has not explicitly overruled that precedent.

Takeaway. *Jones* held that the government conducts a Fourth Amendment search when it obtains information through a physical trespass. 565 U.S. at 404-05. So, if the government physically intrudes upon private property without consent to conduct surveillance, it must satisfy the Fourth Amendment's warrant requirement or an exception thereto. Short of physically connecting a GPS monitor to a suspect's vehicle, or entering the curtilage of private property without invitation, *see Florida v. Jardines*, 569 U.S. 1 (2013), it is not entirely clear what amounts to a physical intrusion. For example, is the electronic intrusion accomplished by having the phone company activate a cell phone's command center so that it transmits its location information a trespass?

Even if the government's activities in this realm are not a physical intrusion, they may nonetheless interfere with a person's reasonable expectation of privacy under the formulation established in *Katz v. United States*, 389 U. S. 347 (1967), for evaluating whether a search has occurred. Factors important to this analysis include the manner in which the location information was obtained (proactively sending a signal to the phone arguably is a greater intrusion than collecting information based on its connection to a cell tower), the length of the surveillance (the shorter the period, the less the monitoring reveals about the whole of a person's movements), the area in which the surveillance occurred (surveillance of a cell phone's travels along public roadways may not violate a person's reasonable expectation of privacy whereas surveillance that places a cell phone in a private area, such as a home, may). *See, e.g.*, *United States v. Karo*, 468 U.S. 705 (1984) (determining that the government conducts a Fourth Amendment search when it employs a beeper to determine whether an object is inside a private residence).

Given the paucity of definitive guidance, the government is well-advised for all such searches to heed the federal district court's guidance in *Howard*: "That this search is presently found to be permissible, does not make it advisable. Law enforcement would be well-advised to avoid the risk illustrated in this case by getting a warrant . . . ." *Howard*, 426 F. Supp. 3d at 1258 n.9.