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

Posted on Sep. 28, 2020, 10:36 pm by Shea Denning

Two years have passed since the Supreme Court held in *Carpenter v. United States*, 585 U.S. ___, 138 S.Ct. 2206 (2018), that the government carried out a Fourth Amendment search when it obtained historical cell site location information (CSLI) for the defendant's phone from a wireless carrier. Relying 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, the court determined that allowing the government access to at least seven days of historical cell-site records contravenes that expectation, even when the records are generated for commercial purposes and held by a third party.

The *Carpenter* majority characterized its decision as "a narrow one" and noted that it was not expressing a view on "real-time CSLI or 'tower dumps,'" disturbing the traditional application of the third-party doctrine, or "call[ing] into question conventional surveillance techniques and tools, such as security cameras." *Id.* at 2220. Dissenting justices, in contrast, characterized the court's reasoning as "fractur[ing] two fundamental pillars of Fourth Amendment law," and "guarantee[ing] a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely." *Id*. at 2247. (Alito, J., dissenting).

Lower courts have applied and distinguished *Carpenter* in a number of cases involving electronic surveillance and the obtaining of location and other types of information from third parties. This post, the first in a three-part series, summarizes post-*Carpenter* decisions relating to surveillance by pole camera and tower dumps. The second post in this series will examine post-*Carpenter* rulings on the obtaining of real-time surveillance through GPS or CSLI. The third post will consider the use of cell site simulators and the obtaining of other information about a person's on-line activities or accounts from third parties. After reading all three, you can decide for yourself whether *Carpenter*'s progeny has bolstered the majority's view of its limitations or has borne out the dissent's warnings regarding its reach.

Pole Cameras. We've blogged before (here, here, here) about the use of pole (or stationary) cameras. While there is little debate that such cameras may be used in public areas, the use of pole cameras to monitor otherwise private areas like the curtilage of a person's home is subject to significant debate post-*Carpenter*.

***United States v. Moore-Bush*, 963 F.3d 29 (1st Cir. 2020).** I wrote here about the federal district court's ruling in United States v. Moore-Bush, 381 F.Supp.3d (D. Mass. 2019), that the use of a pole camera to monitor a suspect's driveway and the front of her house was a search. The First Circuit in *United States v. Moore-Bush*, 963 F.3d 29 (1st Cir. 2020), reversed on the basis that the trial court violated the doctrine of stare decisis in suppressing evidence obtained from the pole camera. The appellate court said the issue was controlled by factually indistinguishable pre-*Carpenter* First Circuit precedent, *United States v. Bucci*, 582 F.3d 108 (1st Cir. 2009), which was not overruled by *Carpenter*. The appellate court further explained that the district court below "transgressed a fundamental Fourth Amendment doctrine not revoked by *Carpenter*," namely "that what one knowingly exposes to public view does not invoke reasonable expectations of privacy protected by the Fourth Amendment." *Id*. at 32. Pole cameras are, the court reasoned, the "exact kind" of "'conventional surveillance technique'" that *Carpenter* said it was not calling into question. *Id.* at 40. A concurring judge urged the Circuit to use the case to reconsider the *Bucci* holding en banc to determine whether "the result that it requires is one that the Supreme Court's decisions, from *Katz* to *Carpenter*, prohibit." *Id*. at 58 (Barron, J., concurring).

***People v. Tafoya*, 2019 WL 6333762, __ P.3d __ (Colo. App. 2019) (not released for publication), *cert. granted*, 2020 WL 4343762 (Colo. June 27, 2020).** The Colorado Court of Appeals determined in *People v. Tafoya* that the continuous three-month use of a camera mounted to a utility pole to surveil and record the area surrounding the defendant's home, including an area behind his privacy fence, was a Fourth Amendment search. Because the police installed the camera across the street from the defendant's property without first obtaining a warrant and subsequently used the footage to obtain a search warrant for the

defendant's property, the appellate court held that the evidence recovered from the search of the property should have been suppressed.

Law enforcement officers mounted the camera in *Tafoya* after learning that the defendant's home was a possible drug stash house. Detectives could watch the footage from the police station, where they could pan and zoom the camera. The camera provided a view of the portion of the defendant's driveway behind a six-foot privacy fence, which could not be seen from the sidewalk or street. By observing this area of the driveway, officers saw the defendant removing items from vehicles that drove in the driveway.

The government argued that a person could see this area of the driveway from two vantage points: by peering through (from the next-door neighbor's property) thin gaps in the privacy fence or by standing in a particular spot on the exterior stairway of an apartment building behind the defendant's home. And, of course, an officer or anyone else situated at the top of the utility pole where the camera was located could have observed the area with binoculars or other equipment similar to the mounted camera.

The Colorado Court of Appeals reasoned that the lessons from the *Jones* concurrences and *Carpenter* is that "'not all governmental conduct escapes being a 'search' simply because a citizen's actions were otherwise observable by the public at large." *Id*. at *7. And even though *Carpenter* did not call into question surveillance by security cameras, the court cited the district court's decision in *United States v. Moore-Bush* as support for the notion that a pole camera "'is not a security camera by any stretch of the imagination.'" *Id*. at *8. In addition, the court disagreed with the notion that CSLI tracking is more invasive than video surveillance of a person's home: "Visual video surveillance spying on what a person is doing in the curtilage of his home behind a privacy fence for months at a time is at least as intrusive as tracking a person's location — a dot on a map — if not more so." *Id.*

The court was not persuaded by the government's arguments that the area of the defendant's driveway behind his privacy fence hypothetically could be seen through a small gap in the privacy fence, from the private outdoor stairway of the adjacent apartment building or from another elevated vantage point. That argument, the court said, ignored the probability that a viewer could be situated in any of those areas for three months at a time. And crediting it would, in the court's view, mean there was no time limit on how long the police could have continued the surveillance of the defendant's property.

Takeaway. The lawfulness of monitoring otherwise private areas by pole camera remains a topic about which there is significant debate. Factors important to consider in analyzing whether this type of surveillance intrudes upon a person's reasonable privacy interest include the area surveilled, the length of time the area is surveilled and whether the equipment used for surveillance is of the type

generally available to the public (see *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.")

Tower Dumps. When a wireless service provider upon the government's request provides a report of the telephone numbers that connected to a particular cell tower during an identified period of time, it performs a tower dump. Tower dumps can be a very effective tool for law enforcement. Several years ago, they helped the FBI identify two men known as "the High Country Bandits" who robbed more than a dozen rural banks in Arizona and Colorado. The FBI obtained tower dumps for the four most rural robbery locations, ran the numbers through a database, and found only a single number at the site of all four robberies. They then identified a second number that had registered with two of the towers. Voila. They had their suspects. Privacy advocates have expressed concern about what happens to all of the other numbers that are dumped into the government's hands. (In the High Country Bandit case, that amounted to more than 150,000 numbers).

To obtain this information, the Stored Communications Act requires that the government obtain a court order based on reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation. *See* 18 U.S.C. Section 2703. This standard is lower than the standard of probable cause required for issuance of a search warrant. The question post-*Carpenter* is whether a tower dump, which reveals historical location information for individuals' cell phones, and, thus, presumably the individuals who own (or at least use) those phones, is a Fourth Amendment search. *See Carpenter*, 585 U.S. ___, 138 S. Ct. 2206 (2018) (Gorsuch, J., dissenting) (questioning why, under the majority's reasoning a tower dump isn't the "*paradigmatic* example of 'too permeating police surveillance' and a dangerous tool of 'arbitrary' authority"). If so, then a court order under the Stored Communications Act is insufficient and a warrant generally is required.

I found only two post-*Carpenter* cases addressing whether obtaining a tower or network dump is a Fourth Amendment search. In each instance, the court determined that it was not.

***Commonwealth v. Dunkins*, 229 A.3d 622 (Pa. Super. 2020), a*ppeal granted*, 2020 WL 4462644 (Pa. Aug. 4, 2020).** In *Dunkins*, the Superior Court of Pennsylvania considered whether the trial court erred in refusing to suppress wireless internet connection records obtained by campus police without a warrant. The police were investigating a dorm-room robbery perpetrated by two men wearing ski masks in which the robbers assaulted the residents of the dorm. They asked a campus employee to compile a list of the students logged on to the network near the wireless access point in the dorm at the time of the robbery. Only

three people were logged on who did not live in the dorm. Two were female and the other was the defendant, a student at the college who lived in another dorm. One of the residents at the dorm told police that the defendant had previously taken marijuana from him without payment. After other evidence linked the defendant to the robbery, he was arrested and charged. He moved to suppress the evidence on the basis that the campus police conducted an unlawful search by obtaining the campus WiFi log-on data without first obtaining a warrant. The trial court denied the motion, and the defendant was convicted and appealed.

The appellate court rejected the defendant's argument that the disclosure of the network access log was a search under *Carpenter*. The court noted that *Carpenter* did not invalidate "tower dump" requests and that the police action in this case was akin to a tower dump. Campus police did not target a specific individual or attempt to track a person's movements; instead, they merely sought to ascertain who was logged on to the WiFi at the time of the robbery. Unlike CSLI, which tracks a phone's (and thus an individual's) movement at all times of the day, the WiFi data disclosed in *Dunkins* was collected only when a person logged onto the campus network and was present on the campus. In addition, the court concluded that the defendant consented to the college's internet use policy, which authorized the college to collect and disclose internet data received through its network connections.

***United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (per curiam).** The Seventh Circuit in Adkinson considered whether the trial court erred in denying the defendant's motion to suppress information that T-Mobile gave to law enforcement about the location of the defendant's cell phone during robberies of T-Mobile and other cell phone stores. In investigating the robbery of a T-Mobile store in Indiana and a Verizon store in Kentucky, T-Mobile conducted its own tower dumps. It pulled data from cell sites near the stores to identify which phones connected to them at the time of the robberies. From this data, T-Mobile determined that the defendant's phone was the only T-Mobile phone near both robberies. T-Mobile voluntarily gave this information to the FBI.

The defendant argued that the evidence should have been suppressed because the government obtained it without a warrant. The trial court denied the defendant's motion. He was convicted at trial and appealed.

The Seventh Circuit affirmed the district court's judgment, rejecting the defendant's argument that the government's acquisition of the tower dump data violated the Fourth Amendment. The court reasoned that T-Mobile was a private party that was not acting as a government agent when it collected the data and turned it over to the government. Instead, T-Mobile was acting in its own interest to prevent more robberies of its stores and to recover its property. In addition, the court reasoned that the defendant consented to T-Mobile collecting and sharing his cell-site information, pursuant to T-Mobile's policy that it could

disclose that information when necessary to protect its rights, interests, property, or safety, or that of others. And, finally, the court noted that *Carpenter* did not advance the defendant's argument as it did not invalidate warrantless tower dumps.

Takeaway. It remains unclear whether the government's obtaining of tower dump information from a third-party intrudes upon a person's reasonable expectation of privacy or instead is covered by the third-party doctrine. On the one hand, tower dumps reveal the same sort of involuntarily submitted location information at issue in Carpenter and they sweep up vast amounts of data. On the other hand, tower dumps generally cover a very limited period of time and do not provide the type of historical tracking that reveals the whole of a person's movements. As both *Dunkin* and *Adkinson* involved the data collectors searching their own records, neither resolves the constitutional questions surrounding tower dumps performed at the behest of the government.