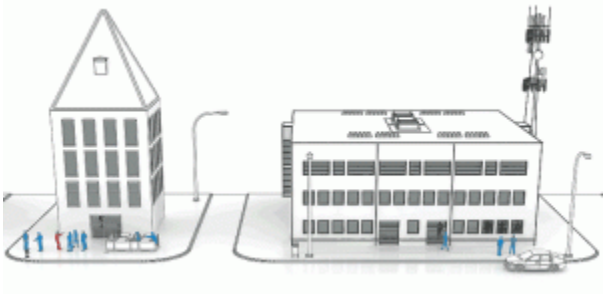
Conducting Surveillance and Collecting Location Data in a Post-Carpenter World, Part III

Posted on Oct. 12, 2020, 5:09 pm by Shea Denning

This post is the third 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 summarized post-*Carpenter* decisions relating to surveillance by pole camera and tower dumps. The second examined 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). This post examines the use of cell site simulators and the obtaining of other information about a person's on-line activities or accounts from third parties.



Jemal R. Brinson, Cell site simulators: How law enforcement can track you, Chicago Tribune (Feb. 18, 2016).

Cell site simulators. Cell site simulators (also called Stingrays or Hailstorms) mimic cell phone towers by producing a boosted signal that "muscles out the signals from legitimate cell towers," becoming the "preferred signal source" for cell phones in the area, thereby forcing them to connect. *See* Adam Bates, *Stingray: A New Frontier in Police Surveillance, Policy Analysis No. 809* (Cato Institute Jan. 25, 2017), available at https://www.cato.org/publications/policy-analysis/stingray-new-frontier-police-surveillance [hereinafter *A New Frontier*]; see also *Stingray Tracking Devices: Who's Got Them?*, (ACLU Nov. 2018), available at https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them; *Cell-Site Simulators/IMSI Catchers*, (Electronic Frontier Foundation Aug. 28, 2017), available at https://www.eff.org/pages/cell-site-simulatorsimsi-catchers. When a phone connects to the cell site simulator, it shares an identifying signal (and perhaps more) with the device. *See* Bates, *A New Frontier*. The phone's location can then be identified with precision (reportedly within six feet of accuracy). *Id*. Indeed, law enforcement officers have used the devices to identify a phone within a particular section of a large apartment building. *See id.* (citing *United States v. Rigmaiden*, 844 F. Supp.2d 982, 996 (D. Ariz. 2012)).

Before *Carpenter*. Before *Carpenter*, the Circuit Court of Appeals for the D.C. Circuit held in *Jones v. United States*, 168 A.3d 703 (D.C. Cir. 2017), that the use of a cell site simulator to locate the defendant's phone (and thus, the defendant) was a Fourth Amendment search. In *Jones*, law enforcement officers used a truck equipped with a cell site simulator to locate the defendant whom they suspected of sexually assaulting and robbing (in separate events over a two-day period) two women who had advertised escort services. The morning following the second incident, officers obtained cell site location information for the suspect's and one of the victim's phones that suggested the phones were in the vicinity of a metro station. The officers took the simulator-equipped truck to the metro station. Once there, they tracked the signal to a parked car, where they located the defendant, his cellphone, the victims' cellphones, and other evidence. The defendant moved to suppress the evidence on the basis that the stingray search was unlawful. The trial court denied the motion and the defendant appealed.

The D.C. Circuit concluded that the use of the cell site simulator to locate the defendant's phone invaded a reasonable expectation of privacy. First, the court noted the potential for location information gathered by a cell site simulator to reveal sensitive, personal facts. Nevertheless, given the Supreme Court's determination in *United States v. Knotts*, 460 U.S. 276 (1983), that the use of a beeper to track a suspect's movements in public spaces did not invade a reasonable expectation of privacy, and without the benefit of the yet-to-be-decided *Carpenter*, the *Jones* Court determined that this intrusion was insufficient by itself to support a conclusion that the government had invaded a reasonable expectation of privacy. What tipped the balance for the court was the *method* by which the government obtained the information. The government determined where Jones was by using "a powerful person-locating capability that private actors do not have" — methodology that was quite different from visually tracking an already identified subject. *Id.* at 712 (noting that a cell site simulator can be used by the government not merely to *track* a person but to *locate* him or her). In addition, the court noted that the simulator worked by exploiting a security flaw "in a device that most people now feel obligated to carry with them at all times." *Id*. at 714. The court reasoned that "[a]llowing the government to deploy such a powerful tool without judicial oversight would . . . 'shrink the realm of guaranteed privacy' far below that which 'existed when the Fourth Amendment was adopted.'" *Id*. (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). It also would force a person to either (a) accept the risk that his or cell phone might at any moment be converted into a tracking device or (b) forgo use of a device necessary to function in modern society. Thus, the court concluded that "under ordinary circumstances," the use of a cell site simulator to locate a person through his or her cell phone invades the person's reasonable expectation of privacy in his or her location information. *Id*. at 714-15.

Jeff Welty wrote here about *Jones* and two other pre-*Carpenter* cases holding that using a cell site simulator was a search.

After *Carpenter*. In *State v. Sylvestre*, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018), the District Court of Appeal of Florida held that the government was required to obtain a warrant or satisfy an exception to the warrant requirement before using a cell site simulator. In *Sylvestre*, the defendant was charged with first-degree murder arising form the robbery of a restaurant. Investigators received cell site location information for the defendant's phone, which narrowed down his location to several square blocks. An officer then used a cell site simulator (without a court order) to pinpoint the residence in which the defendant's phone was located. The appellate court reasoned that if a warrant is required for the government "to obtain historical cell site location information voluntarily maintained and in the possession of a third party," it must be required for "the more invasive use of a cell-site simulator." *Id.* at 991. The court said this was "especially true when the cell phone is in a private residence" or another private location, including "'doctor's offices, political headquarters, and other potentially revealing locales.'" *Id*. (quoting *Carpenter*, 138 S. Ct. at 2218).

Takeaway. It seems highly likely following *Carpenter* that the use of a cell site simulator is a search under the Fourth Amendment. Cell site simulators intercept signals from cell phones without the users' consent, they interrupt service for the affected phones (*see Jones*, 168 A.3d at 708 n.7, 710 & n. 15), and they reveal precisely where the phones are located.

Other third-party information. Though the Supreme Court in *Carpenter* said its decision was a narrow and that it was not disturbing the application of the third-party doctrine, dissenting justices accused the court of rendering the third-party doctrine "unprincipled and unworkable." 134 S. Ct. at 2224 (Kennedy, J., dissenting). Noting that the Court's holding was premised on cell site records being a "'distinct category of information'" from other business records, Justice Kennedy criticized the majority for failing to explain what makes certain types of records a distinct category. *Id*. at 2234 (Kennedy, J., dissenting). He listed the following as "just a few of the difficult questions that require answers" after *Carpenter*:

- Whether credit card records are distinct from bank records;
- Whether payment records from digital wallet applications are distinct from either credit card records or bank records;
- Whether the electronic bank records available today are distinct from the paper and microfilm records at issue in *United States v. Miller*; and
- Whether cell-phone call records are distinct from the home-phone call records at issue in *Smith v. Maryland*.

Id. (Kennedy, J., dissenting).

To date, courts have not identified additional exceptions to the third party doctrine (discussed here) based on *Carpenter*. (Even before *Carpenter*, courts had recognized that persons retain a privacy interest in content information held by third parties. *See, e.g, Ex parte Jackson,* 96 U.S. 727, 733 (1878) (noting that while a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause); *United States v. Warshak,* 631 F.3d 266, 283–288 (6th Cir. 2010) (extending the privacy protections afforded to mailed and telephonic communications to the content of e-mails held by internet service provider).) Thus, courts have upheld the warrantless disclosure of records related to the following:

- Bitcoin transactions, *see United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020)
- Internet protocol addresses, *see* United States v. Morel, 922 F.3d 1 (1st 2019)
- Facebook registration information, billing records, and session times and durations, *see United States v. Cox*, ___ F. Supp. 3d ___, 2020 WL 2899685 (N.D. Ind. June 3, 2020).

Of course, *Carpenter* is of recent vintage, the composition of the court has changed since it was decided, and the well of information in the hands of third parties is deep. So there are apt to be future developments. Courts considering whether to carve out exceptions to the third-party doctrine for other categories of records will be called upon to consider whether the records resulted from an individual sharing — out of some necessity — an "intimate window into [his or her] life," see *Carpenter*, 138 S. Ct. at 227, or, in contrast, whether the records are created through a person's affirmative and voluntary acts.