Fourth Circuit Says Law Enforcement Doesn't Need a

Digital Media and Data Privacy Law Blog

on 06.06.2016
Posted in Privacy

Like many people, Aaron Graham and Eric Jordan carried cell phones around in 2011. Unlike most people, Graham and Jordan were convicted of crimes arising from their participation in a series of armed robberies[1] in that period, and were soon sorry that they had their cell phones on them when those robberies happened. Sitting *en banc*, the U.S. Court of Appeals for the Fourth Circuit just made them sorry last Tuesday in *United States v. Graham*, No. 12-4659 (4th Cir. May 31, 2016).

Because in their investigation, federal agents sought the cell-site location information (or "CSLI" as the kids say these days) for Jordan and Graham to establish their presence in the general vicinity of the robberies. That is, cell phones rely on proximity to their providers' cell towers to get signals, and the providers (Verizon, Sprint, etc.) generally keep records of which phones are linking up to which towers at any given moment. Those records are the CSLI, and those are what the agents wanted to get to build their case.

And the Stored Communications Act says the agents were allowed to get that information, even without a warrant. Specifically, the Act says that to get access to these records, the government needed to demonstrate either (1) probable cause for a warrant, or (2) specific and articulable facts showing reasonable grounds to believe that the records are relevant and material to an ongoing criminal investigation for a court order. 18 U.S.C. § 2703(c), (d). Here, the agents followed the second route and got a court order but not a search warrant. The Defendants didn't claim the government violated the statute, but did argue that the statute violated the Fourth Amendment's protections against unreasonable searches and seizures.

The defendants tried to put their case in a box with others where the government unconstitutionally collected private information. In *United States v. Karo*, 468 U.S. 705, 714-15, (1984), for instance, the Drug Enforcement Agency placed a beeper within a can of ether and received tracking information from the beeper while the can was inside a private residence. Similarly, in *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001), the Department of the Interior used a thermal imager to gather "information regarding the interior of the home." And in *United States v. Jones*, 132 S. Ct. 945, 948-49, 954 (2012), the FBI and local law enforcement secretly installed a GPS tracking device on a suspect's vehicle and monitored the vehicle's movements for four weeks.

The Fourth Circuit didn't view collection of the cell-site information the same way. Instead, the court looked at it as information voluntarily turned over to a third party under *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). Under that rule – the third-party doctrine – an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party. *Id*. That is, by "revealing his affairs to another," an individual "takes the risk . . . that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 443 (1976).

The rule applies even when "the information is revealed" to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id*.

Graham and Jordan argued that they hadn't voluntarily turned over their location information at all, and that cell phone users don't even possess the CSLI to convey it to anyone. The court didn't buy it and wrote:

Anyone who has stepped outside to "get a signal," or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters. . . . Whenever he expects his phone to work, he is permitting -- indeed, requesting – his service provider to establish a connection between his phone and a nearby cell tower. A cell phone user thus voluntarily conveys the information necessary for his service provider to identify the CSLI for his calls and texts.

In reversing its panel decision on this issue, the Fourth Circuit defuses a circuit split the panel created last August in *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015). It now sits in accord with the Sixth, Eleventh, Fifth, and Third Circuits in holding that collecting this cell-site information in compliance with the Stored Communications Act but without a warrant does not violate the Fourth Amendment.

If you are considering committing a bunch of crimes that require your physical presence in a particular place, consider leaving your cell phone at home. Law enforcement will be able to figure out where you were, and it won't need a warrant to do it.

---

[1] One of the places robbed was a Dollar Tree store in Baltimore County, so I remind you not to be poor in the United States, as it often leads to terrible situations like this.