Fourth Circuit: Cell Site Location Information Requires a Search Warrant

Author : Jeff Welty

Categories : Evidence, Search and Seizure

Tagged as : CSLI, digital evidence, graham, stored communications act

Date : August 10, 2015

The Fourth Circuit just decided *United States v. Graham*, an important case about law enforcement access to cell site location information (CSLI). This post summarizes the case, explains its importance for North Carolina proceedings, and puts it in context in the broader debate about this type of information.

Facts. Defendants Graham and Jordan committed a string of armed robberies of Baltimore businesses. They were arrested as they drove away from one of the crimes. Their cell phones were in the truck they occupied. In an effort to link the defendants to the other robberies, officers sought court orders under 18 U.S.C. § 2703(d), a provision in the federal Stored Communications Act, for historical records regarding the phones.

Under the statute, such orders may be issued based on a showing akin to reasonable suspicion and less than probable cause. Using this standard, the officers ultimately obtained two sets of orders, one that covered a total of 14 days, scattered around each of the previous robberies, and one that covered a continuous seven-month period encompassing all of the robberies. Sprint produced records in response to the orders, including cell site location information (CSLI) that placed the defendants at or near the locations of most of the robberies.

Procedural history. The defendants were charged with assorted federal crimes. They moved to suppress the CSLI, arguing that the officers engaged in an unreasonable search when they obtained that information without a full-fledged search warrant based on probable cause. The district court judge denied the motion to suppress, the defendants were convicted on all counts, and they appealed.

Majority opinion. The Fourth Circuit panel assigned to hear the case split 2-1, with a majority agreeing with the defendants that the CSLI was obtained through an unreasonable warrantless search. Judge Davis wrote the majority opinion, which Judge Thacker joined. The majority first reviewed how CSLI is generated and stored, and then explained that it may be accessed using court orders under the Stored Communications Act. The majority then gets down to business, holding that accessing such information is a Fourth Amendment search because it intrudes upon a reasonable expectation of privacy, and that doing so without a full probable cause search warrant or an exception to the warrant requirement is constitutionally inadequate:

> [T]he government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information. Its inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies.

The majority rejected the idea that Sprint's terms of service, which allow it to collect certain customer data including location information, remove any expectation of privacy regarding the CSLI. Further, it supported its reasoning regarding expectations of privacy by emphasizing that CSLI is generated even when a phone subscriber is in his or her

home or another private location. Finally, it noted that in the GPS tracking case, United States v. Jones, __ U.S. __, 132 S. Ct. 945 (2012), five Justices expressed the view that long-term GPS tracking would violate a reasonable expectation of privacy. Although CSLI is not as precise as GPS, the majority thought that Jones was still relevant, noting that CSLI was precise enough to help convict the defendants.

Crucially, the majority rejected the government's argument that CSLI falls under the third-party doctrine of Smith v. Maryland, 442 U.S. 735 (1979) (finding no reasonable expectation of privacy in telephone numbers dialed by a suspect, as those numbers were voluntarily provided by the suspect to a third party, namely, the phone company). The majority acknowledged that the CSLI was available only because of the defendants' voluntary use of their phones, but opined that the information was generated by Sprint rather than being voluntarily conveyed to Sprint by the defendants:

> We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person. Cell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic participation. . . . People cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones.

Scope of the ruling. Although the opinion concerns historical CSLI, the majority's reasoning clearly also applies to the prospective or real-time collection of CSLI. However, the majority limited its holding to instances when law enforcement obtains CSLI covering "an extended period of time." It characterized even 14 days -- the duration of the shorter orders obtained in this case -- as "extended," but specifically declined to draw a bright line defining extended collection, and did not analyze the status of, for example, an order allowing law enforcement to access to 24 hours of CSLI.

Good faith, bad news. While the foregoing may sound like good news for the defendants, it wasn't. The majority ruled that the officers acted in good faith in obtaining the CSLI under the Stored Communications Act and pursuant to the orders of two federal magistrate judges, and so affirmed the denial of the defendants' motion to suppress.

Dissenting opinion. Technically, Judge Motz's opinion is a concurrence in the judgment, as she, too, would have affirmed the defendants' convictions. But on the CSLI issue, her opinion reads like a dissent, arguing that the majority opinion "flies in the face of the Supreme Court's well-established third-party doctrine." She distinguishes the GPS tracking and beeper cases as involving the surreptitious collection of location information by the government, while in this case the government sought only records already generated by Sprint. Further, she argued that a subscriber voluntarily conveys his or her location to a service provider by using, or even turning on, his or her phone: "Defendants . . . 'assumed the risk' that the phone company would disclose their information to the government." The dissent also points out that the greater weight of federal authority favors the application of the third-party doctrine.

Context. There is an increasing body of case law on the constitutional status of CSLI. I summarized the major cases in Chapter Three of my book *Digital Evidence*, but the nutshell version is that the Fifth and Eleventh Circuits have ruled that the third-party doctrine applies to CSLI so there is no reasonable expectation of privacy in it and no warrant needs to be obtained to get it, *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013), while the Third Circuit has issued a rather murky opinion more or less agreeing with that perspective but ruling nonetheless that a court may sometimes require a warrant before compelling access to CSLI, *In re Application of the U.S.*, 620 F.3d 304 (3d Cir. 2010), and now the Fourth Circuit has joined several state and lower federal courts in ruling that CSLI is often protected by the Fourth Amendment and subject to the warrant requirement. My rough sense of the state of affairs is that there is still a greater weight of authority in favor of applying the third-party doctrine, but momentum is on the side of finding a reasonable expectation of privacy in CSLI. Obviously, things are fluid.

Next steps. The Fourth Circuit could rehear the case en banc. The defendants might petition for it, since their convictions and sentences were affirmed, or the government might, since it won overall but lost on a key issue. After

any en banc review, the Supreme Court could weigh in on this issue, either in this case or in another one that presents the same basic question. If the Fourth Circuit were to take the case en banc and reverse the panel, the likelihood of Supreme Court review would be reduced as that would mostly remove the circuit split.

Impact on North Carolina proceedings. The Fourth Circuit's rulings don't directly bind the North Carolina courts, but this case is still a big deal for North Carolina proceedings. First, it may be viewed as persuasive authority by North Carolina judges, who might refuse to issue less-than-probable-cause court orders for CSLI, or who might suppress evidence obtained using such orders. (There is currently no North Carolina appellate case law on this issue so trial court judges are on their own.) Second, it is important to officers who are investigating cases that could be adopted for federal prosecution. To preserve the option of seeking federal prosecution, an officer will need to comply with the procedures that the federal courts require. In short, this case further bolsters the advice I gave previously in my book: "[T]he safest course for law enforcement officers is to procure a search warrant when seeking location information."

Further reading. Both the majority and the dissenting opinions are detailed and thoughtful and are worth a read. Further context on this issue is available in my book. Further ruminations about the impact of this case from Professor Orin Kerr are available here.