Court Rules that Warrant Is Required for Stored Cell Site Location Information

by Greg Nojeim [1]
September 12, 2011

A Federal District Court in New York ruled [2] on August 22, 2011 that a warrant is required for law enforcement access to *stored* cell site location information generated by the operation of a cellular phone. Judge Nicholas G. Garaufis rejected the government's application for an order under Section 2703(d) of the Electronic Communication Privacy Act, which requires only that the government prove by use of "specific and articulable facts" that the location information sought is relevant and material to a criminal investigation. Instead, the court determined that requiring a cell phone service provider to produce retrospective location information about the movements of a suspect (and his cell phone) over a 113-day period required a showing of probable cause. Said the court:

> The advent of technology collecting cell site location records has made continuous surveillance of a vast portion of the American populace possible: a level of Governmental intrusion previously inconceivable. It is natural for Fourth Amendment doctrine to evolve to meet these changes.

The case, captioned *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, stands out for a couple of reasons. First, most courts requiring probable cause for law enforcement access to location information have been considering requests for *prospective* location information that would allow tracking of a person in real time. This court was considering an application for access to *stored* or "retrospective" location information about a person's movements in the past. While the Third Circuit Court of Appeals ruled [3] last year that magistrates have discretion to require probable cause warrants for stored location information, Judge Garaufis went further, ruling that a probable cause warrant is *required* for law enforcement to compel a provider to turn over this information.

Second, the court made a strong case for excepting cumulative cell site location records from the third party disclosure doctrine. Under that doctrine, once a person voluntarily discloses information to a third party – like the numbers dialed on a telephone when making a call, or check and deposit slips given to a bank – the person relinquishes any Fourth Amendment interest the person may have had in the information conveyed to the third party. See *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976).

The court found that there is a "content exception" to the third party doctrine, and that cumulative cell site location records are sufficiently sensitive that a similar exception should be created for those records. It said that that this content exception explained why the contents of First Class Mail are protected by the Fourth Amendment though that mail is conveyed through the Postal Service, and why the Court in *Smith v. Maryland* determined that numbers dialed on a telephone and conveyed to the telephone company when making a call were not Fourth Amendment protected even though call content – also conveyed to the phone company – is protected. For the bridge from call content to email content, the court relied in part on *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010) – the first circuit court decision to hold squarely that the Fourth Amendment fully protects email content and that a warrant is required for law enforcement access. For the bridge from content to location information, the court relied in part on *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), which held that that a people have a reasonable expectation of privacy in the totality of their movements over a lengthy period of time – 30 days, in that case – even if they don't have a reasonable expectation of privacy in a single movement from one point to another. (The Supreme Court will hear the government's appeal of the *Maynard* decision this fall, under the name *U.S. v. Jones*.) The court indicated that the privacy interest at stake in this case was even greater because that case involved tracking a person while in his vehicle; cell phones are with the user all the time, enabling tracking of a person regardless of whether the person is in a vehicle. It then concluded that

cumulative cell site location information records, like call content, “implicate sufficiently serious protected privacy concerns” that an exception to the third party disclosure rule is warranted.

This, of course, raises questions about what other types of information provided voluntarily to a third party implicate sufficient privacy concerns that they, too, should be excepted from the third party doctrine. The court left discussion of those matters to another day.

The decision adds to the weight of case law [4] supporting reforms sought by the Digital Due Process coalition [5]. One of those reforms would require warrants for both prospective and stored location information. The case could give a boost to that call for reform, and to the GPS Act, S.1212/H.R. 2168, a bill introduced by Senator Wyden (D-OR) and Reps. Goodlatte (R-VA) and Chaffetz (R-UT) to require warrants for cell site, GPS and other location information. It might also encourage Senator Leahy (D-VT) to require warrants for stored location information in the ECPA Reform Act, S.1011, which currently requires warrants for prospective location information, but not for stored location information.

Links:
[1] https://cdt.org/personnel/greg-nojeim
[2] http://ia600309.us.archive.org/33/items/gov.uscourts.nyed.312774/gov.uscourts.nyed.312774.6.0.pdf
[3] http://www.ca3.uscourts.gov/opinarch/084227p.pdf
[4] http://www.cdt.org/blogs/joshua-gruenspecht/courts-boldly-go-fourth-rulings-validate-digital-due-process
[5] http://www.digitaldueprocess.org