THOMSON REUTERS
Westlaw®

Every step you take: Police's search for armed robber makes new law on privacy of geolocation information

By Jayce Born, Esq., Amanda C. Hoover, Esq., Ronald D. Lee, Esq., and Suneeta Hazra, Esq., *Arnold & Porter Kaye Scholer LLP**

JUNE 3, 2021

An armed robber walks into seven stores in Indiana and Michigan during a three-week crime spree in October 2017. Investigators get from the robber's phone carrier real-time cell site location information (CSLI) that show his phone's pings to nearby cell towers, which help the investigators geolocate their suspect.

The robber gets arrested and charged in federal court with five counts of robbery and several accompanying weapons charges. And the rest of the world gets an opinion from the US Court of Appeals for the Seventh Circuit[1] on one of the many questions that the Supreme Court left open when it decided its seminal privacy-related opinion *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

In this post, we provide a brief overview of the Seventh Circuit's decision before diving into why even those who *aren't* armed robbers should keep an eye out for other cases that might follow in the Seventh Circuit's footsteps.

THE DECISION

On the losing end of the Seventh Circuit's decision was Rex Hammond, the suspected robber who was located by investigators using cellphone pings.

After being convicted of all charges and sentenced to 47 years in prison, he argued to the Seventh Circuit that the district court erred in denying his motion to suppress the real-time CSLI data that investigators used to find him because the collection of that data violated the Fourth Amendment.

The Seventh Circuit disagreed, holding that the collection of real-time CSLI data under these circumstances was not a "search."

The court reasoned that Hammond's case was more like the Supreme Court precedent, *United States v. Knotts*, 460 U.S. 276 (1983), than it was like *Carpenter*. In *Knotts*, law enforcement agents attached a beeper to a drum of chloroform to track its (and the defendants') movements in real time.

In *Carpenter*, on the other hand, the agents collected *historical* CSLI data that essentially revealed the defendant's every move for the prior 127 days.

To the Seventh Circuit, the cellphone pings were like a beeper, and Hammond was like a drum of chloroform: The cellphone pings revealed only his current location and allowed investigators to follow him physically on public roads and in public parking lots for only six hours, without the need for electronic surveillance.

The real-time data didn't provide a "window" into Hammond's personal or non-public life "to the same intrusive degree as the collection of historical CSLI" did in *Carpenter*.

Nonetheless, the Seventh Circuit also ruled in the alternative that law enforcement collected the real-time CSLI in the good faith belief that 18 U.S.C. § 2702 — a provision of the Stored Communications Act that allows telephone providers to disclose records during an emergency — permitted the collection.

> As courts continue to define the information that is and is not protected by the Fourth Amendment's warrant requirement after *Carpenter*, companies should review their privacy, security and legal policies.

Thus, the Seventh Circuit held that the officers' conduct fell within the Fourth Amendment's good-faith exception, under which courts will not suppress evidence seized as the result of an unlawful search.

THE IMPACT

The Seventh Circuit limited its holding to the specific facts at hand, leaving open the possibility of a different result in a case in which the suspect wasn't imminently likely to commit another violent felony. But the opinion is instructive regarding the types of considerations that companies collecting location data should weigh when responding to law enforcement requests for such data.

Of course, traditional electronic communication service providers that collect CSLI know to stay abreast of the legal landscape to recognize when they can and should push back on warrantless law enforcement requests for CSLI. But the near ubiquity of Internet of Things (IoT) devices means that many other types of companies now collect location data akin to CSLI, too.

As courts continue to define the information that is and is not protected by the Fourth Amendment's warrant requirement after *Carpenter* — and, in doing so, weigh in on what type of information about a person's life carries a reasonable expectation of privacy — companies should review their privacy, security and legal policies.

To be sure, many telecommunications carriers, IoT-enabled device manufacturers, and app providers need to know the location of a user's phone or device in order to provide their services, so they may be limited in how they can protect customer data on the front end (through minimization, encryption, or other technical measures).

But for legal, business or individual privacy reasons, companies may resolve to challenge government requests for location data when allowed by law.

In evaluating whether to challenge such requests, companies should assess the considerations outlined in caselaw in their jurisdiction, including the type (i.e., real-time or historical) and amount of CSLI or other geolocation information sought, the types of privacy interests this data might implicate, the exigency of circumstances presented, the government's possession of a warrant or other legal process, and any other relevant information they have.

Notes

[1] https://bit.ly/2RVYFPZ

This article was published on Westlaw Today on June 3, 2021.

ABOUT THE AUTHORS

(L-R) **Arnold & Porter Kaye Scholer LLP** associate **Jayce Born**'s practice focuses on complex civil litigation and defense of government investigations and regulatory enforcement actions. She is resident in the firm's Washington, D.C., office and can be reached at jayce.born@arnoldporter.com. **Amanda C. Hoover**'s practice focuses on civil litigation, internal investigations and regulatory matters. She is an associate in the firm's Washington, D.C., office and can be reached at amanda.claire.hoover@arnoldporter.com. **Ronald D. Lee** advises and represents clients in national security, cybersecurity and privacy cases, as well as government contract matters. A partner in the firm's Washington, D.C., office, he can be reached at ronald.lee@arnoldporter.com. **Suneeta Hazra** counsels clients on internal and government investigations, privacy and cybersecurity matters, and environmental enforcement actions. She is a partner in the firm's Denver office and can be reached at suneeta.hazra@arnoldporter.com. This article originally appeared May 21, 2021, on Arnold & Porter Kaye Scholer LLP's blog, Enforcement Edge. Republished with permission.