LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Open Questions In Unsettled Geofence Warrant Landscape

By **Charles Fowler** (October 7, 2024, 4:52 PM EDT)


Charles Fowler

This summer produced the first two federal appellate decisions on the Fourth Amendment implications of geofence warrants.[1]

A geofence warrant is a controversial new investigative tool that lets agents identify some of the cellphones in a given area at a given time. Geofence warrants have taken off in recent years. Agents have used them to investigate crimes as routine as smashed car windows,[2] and as high-profile as the Jan. 6 riot at the U.S. Capitol.[3]

These early precedents bring little clarity to the emerging issues surrounding geofence warrants. In July, the U.S. Court of Appeals for the Fourth Circuit held in U.S. v. Chatrie that geofence warrants are not a Fourth Amendment search, and thus do not even require a warrant.[4]

The next month, in U.S. v. Smith, the U.S. Court of Appeals for the Fifth Circuit held not only that geofence warrants are a search, but also that they are categorically unconstitutional general warrants.[5]

Neither decision is final. And the dust may well settle somewhere in between these poles: Geofence warrants are likely governed by the same probable-cause, overbreadth, particularity and good faith rules as courts apply to most other warrants. As such, they are likely subject to case-by-case assessment.

But given the unsettled landscape, wise defendants will broadly preserve Fourth Amendment challenges — and develop a favorable factual record — so that they can benefit from new legal developments.

Background on Geofence Warrants

A geofence warrant is a warrant for data about the mobile devices in a given area at a given time. Agents use geofence warrants when they know a crime happened but have no suspects.

Most geofence warrants are directed to Google LLC. They seek data that Google stores in its Sensorvault database for users who enable the location history feature of their Google accounts.[6] Location history lets Google track where a user takes their cellphone. Location history is off by default, and so users must opt in. About one-third of Google users have opted in.[7]

Geofence warrants follow a three-step process. First, agents send Google a geographic area and time

range — a radius around the crime scene for perhaps a half-hour on either side of the crime. Google then produces an anonymized list of accounts that were likely in the area. The data is not perfect.[8]

Second, agents narrow the account list by, for instance, eliminating those not in the target area long enough to have committed the crime. Agents then seek — and Google provides — more location data for the narrowed list. This data is not limited to the area and time range that defined the original request.[9]

Third, using the Step 2 data and information obtained through other investigative processes, agents identify suspect accounts from the narrowed account list. Agents then ask Google to unmask the suspect accounts by providing identifying information.[10]

Geofence warrants have grown in popularity since they emerged around 2016. But Google's policy for storing location history data may soon curtail their use by making it impossible for Google to provide responsive data.[11]

Still, it appears that it will still be at least months until Google implements the changes, and agents are still serving geofence warrants. And since it may take many months for Google to respond to a warrant once served,[12] there may be no imminent end to new geofence cases.

The Fourth and Fifth Circuits' Radically Divergent Approaches

To date, just two federal appellate decisions have addressed geofence warrants. They could hardly diverge more starkly.[13]

In U.S. v. Chatrie, the Fourth Circuit considered a geofence warrant that led to an armed bank robber's arrest.[14] The court affirmed denial of the defendant's suppression motion because he lacked "a reasonable expectation of privacy in the two hours' worth of Location History data voluntarily exposed to Google."[15] Thus, according to the court, the government conducted no Fourth Amendment search.

The Fourth Circuit reasoned that geofence warrants implicate both rationales for denying protection to information exposed to third parties. First, the limited location data obtained through the initial search is more like tracking a short, isolated trip than surveilling all a suspect's movements over a long period; it thus raises little privacy concern.[16] Second, Google does not automatically store location data, but requires a voluntary, affirmative act for users to opt in.[17]

In U.S. v. Smith, in contrast, the Fifth Circuit held that geofence warrants are categorically unconstitutional general warrants.[18] The court first held — contrary to Chatrie — that a geofence warrant is a Fourth Amendment search.

The court reasoned that tracking someone's movements — even for a short time — "is invasive for Fourth Amendment purposes."[19] The court also questioned whether opting into location history is really informed and voluntary.[20]

Next, the Fifth Circuit held that geofence warrants allow a categorically unconstitutional "general, exploratory rummaging."[21] The court focused solely on the first step of Google's three-step process, explaining that Google must "search through its entire database to provide a new dataset that is derived from its entire Sensorvault."[22]

Here, too, the Fifth Circuit parted with the Fourth, which had reasoned that Google conducts this initial, sweeping search, and thus refused to attribute it to the government.[23]

Even so, the Fifth Circuit held that the U.S. District Court for the Northern District of Mississippi correctly applied the good faith exception to the exclusionary rule.[24] Since the agents diligently tried to ensure that their "cutting-edge investigative technique" complied with the Fourth Amendment, the court saw little deterrence benefit to excluding evidence.[25]

Open Questions

Open questions after these cases command vigilance in preserving Fourth Amendment challenges. Neither Chatrie nor Smith is final. Chatrie sought rehearing in August, and Smith's rehearing petition is due in October. Several amici support Chatrie. The en banc votes will be interesting since both panels' broad holdings — on purely legal grounds — may catch other judges' attention.

Whoever ultimately loses these cases may also seek certiorari. But the U.S. Supreme Court is unlikely to weigh in until the lower courts have more fully developed the law governing geofence warrants. The Supreme Court may also wait and see whether Google's policy changes eventually moot the issue.

While the Fourth and Fifth Circuits staked out extreme positions, the rubber may hit the road somewhere in between. There is no obvious reason why courts should not treat geofence warrants like most others, assessing them case by case. Several district courts have taken just this approach.[26]

Given the unsettled landscape, defendants should assert and preserve the full range of conventional Fourth Amendment challenges to geofence warrants.

A court considering a Fourth Amendment challenge to a warrant typically asks whether probable cause existed; whether the probable cause supported the warrant's full scope, i.e., overbreadth; whether the warrant sufficiently described the place to be searched and things to be seized, i.e., particularity; and, if the warrant is invalid, whether agents still relied on it in good faith. Geofence warrants pose novel questions at each step.

How, for instance, must one show probable cause that Google's location data for a given place and time will contain relevant evidence? If only one-third of cellphone users enable location history, it seems likelier than not that a geofence warrant would be unable to identify a lone suspect — though perhaps if evidence showed several suspects, then at least one would probably be identifiable.

Moreover, does probable cause require a particularized showing that the suspect had a cellphone? The warrant applications in both Chatrie and Smith contained some indication that the suspects had phones,[27] but neither court addressed that fact's significance in depth.

On the one hand, the Supreme Court has recognized cellphones' ubiquity in modern life.[28] But, on the other hand, it may be mere speculation that a suspect carried a cellphone — let alone with location history enabled — to commit a crime, especially when it is well-known that police can track it.

Given the circuits' focus on voluntariness, defendants challenging geofence warrants should also explore whether and how they enabled location services. Case-specific facts or expert testimony bearing on voluntariness could strengthen a Fourth Amendment challenge. Indeed, the existing cases suggest that Google maintains at least some location data for those who opted out of location history.[29]

It is unclear — but should be developed in the right case — whether it is possible to catch an opt-out in a geofence warrant.

Finally, defendants may argue that the magistrate exercised too little supervision over the process of mining Google's data. In Smith, for instance, the Fifth Circuit seemed to think the agents were mistaken that the original warrant authorized the whole three-step process of obtaining identifying information, rather than requiring them to apply for a new warrant at each step.[30]

While existing precedents gloss over this new-warrant issue, it could prove dispositive if effectively presented in the right case. After all, it is not the initial request for anonymized data within the geofence's narrow geographic and temporal boundaries, but rather the later request for unbounded and identifying data for some users, that more closely resembles the long-term cellphone tracking at issue in the Supreme Court's 2018 Carpenter v. U.S. decision.[31]

Conclusion

Geofence warrants are a novel innovation in the investigative process. And while Google has said that it will soon curtail their use, geofence cases are unlikely to vanish anytime soon.

What's more, geofence warrants probably foreshadow still more accurate and comprehensive ways to track cellphone users' movements as technology progresses — and as agents devise more creative ways to access it.

Recent circuit precedents raise more questions than they answer about the legal guidelines for geofence warrants, cautioning a comprehensive approach to raising and preserving Fourth Amendment challenges.

Charles Fowler is a principal at McKool Smith. He previously served as an assistant U.S. attorney in the Central District of California and the Western District of Texas.

[1] See United States v. Smith, 110 F.4th 817 (5th Cir. 2024); United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024).

[2] See Smith, 110 F.4th at 822.

[3] See United States v. Easterday, 712 F. Supp. 3d 46, 56 (D.D.C. 2024) (refusing to suppress fruits of the Capitol riot geofence warrant); United States v. Rhine, 652 F. Supp. 3d 38, 90 (D.D.C. 2023) (same).

[4] Chatrie, 107 F.4th at 332.

[5] Smith, 110 F.4th at 838.

[6] Id. at 821-22.

[7] Id. at 823.

[8] Id. at 824-25.

[9] Id. at 825.

[10] Id.

[11] Id. at 823 n.3.

[12] Id. at 825.

[13] The Eleventh Circuit held that a defendant lacked standing to challenge a geofence warrant that identified the defendant's girlfriend's cellphone. United States v. Davis, 109 F.4th 1320, 1331 (11th Cir. 2024). Thus, while the Eleventh Circuit seemed to generally share the Fourth Circuit's view, it did not reach the merits of the defendant's Fourth Amendment claim.

[14] Chatrie, 107 F.4th at 324.

[15] Id. at 325.

[16] Id. at 330.

[17] Id. at 331.

[18] Smith, 110 F.4th at 838.

[19] Id. at 834.

[20] Id. at 835.

[21] Id. at 837.

[22] Id.

[23] Id. at 838 n.12.

[24] Id. at 840 (citing (United States v. Leon, 468 U.S. 897 (1984)).

[25] Id.

[26] Compare, e.g., In re Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62 (D.D.C. 2021) (granting a geofence warrant and detailing the court's reasoning to "add[] to the limited federal caselaw discussing the legality of such warrants"), and In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020) (similar), with In re Search of Info. Stored at Premises Controlled by Google LLC, 542 F. Supp. 3d 1153 (D. Kan. 2021) (holding that there was probable cause that the crime was committed at a place and time, but not that Google would have relevant data within the geofence; also holding that the geofence

boundaries and time period were not sufficiently particularized), and In re Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730 (N.D. Ill. 2020) (holding that a geofence application met neither the probable-cause nor particularity requirements).

[27] See Smith, 110 F.4th at 820; Chatrie, 107 F.4th at 325.

[28] Carpenter v. United States, 585 U.S. 296, 315 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[29] Smith, 110 F.4th at 823.

[30] Id. at 840 n.14. The court held, however, that the good-faith exception excused this error too.

[31] See 585 U.S. at 311-12 (holding that obtaining long-term historical cell site data from a suspect's cellular carrier is a Fourth Amendment search).