Dividing Lines: The Fourth Circuit's Take on Geofence Warrants in United States v. Chatrie Amid Growing Circuit Split

Description

In July 2024, the United States Court of Appeals for the Fourth Circuit issued an opinion in *United States v. Chatrie*, a case that could potentially make its way up to the Supreme Court of the United States, providing the High Court an opportunity to settle an existing circuit split over the constitutionality of geofence warrants as an investigative technique used by law enforcement.[1] Subsequent to the Circuit's July opinion, in November, the Fourth Circuit granted a rehearing en banc to reconsider its earlier decision.[2]

Path of the Guardian: Geofence Warrants and Privacy

Join Path of the Guardian today and gain 12 months of access to weekly training videos. Enroll now to stay ahead and make a lasting impact in your community!

As a brief background, a geofence warrant is a law enforcement tool that requests data from technology companies regarding all devices located within a specific geographic area during a particular time frame. Unlike traditional warrants that specify the person, place, or thing to be searched, geofence warrants are used when the identity of a suspect is unknown. Often referred to as "reverse-location warrants," these warrants start with a location and time and seek to identify the individuals who were present within a specified area of a crime scene.

The *Chatrie* case arose in the wake of a robbery committed in 2019 at the Call Federal Credit Union in Midlothian, Virginia. On the day of the incident, by the time law enforcement arrived on the scene, the suspect had fled westward, supposedly unarmed and carrying $195,000 stolen from the bank's vault. When Detective Hylton arrived at the scene, he initiated witness interviews and undertook a review of the bank's security footage. However, these investigative techniques proved fruitless, as they failed to expose the suspect's identity. While the detective managed to pursue two potential leads, the results were underwhelming as they led to two dead ends. With no other leads to pursue, nor any additional evidence to consider, the detective delved deeper into the little evidence he had. Reflecting on his earlier review of the bank's security footage, he remembered that the suspect had carried a cell phone during the robbery. Recollection of this fact led the detective to request and successfully obtain a geofence warrant from the County Circuit Court.

For Fourth Amendment purposes, the scope and subject matter included within the warrant are important in analyzing this case. Here, the detective's warrant proposed a geofence that included the bank and encompassed a 150-meter radius relative to the bank's location.

The warrant also detailed the three-step process law enforcement expected to use in attempting to obtain the location data from Google. First, Google provides anonymized Location History data for all devices within the geofence from 30 minutes before to 30 minutes after the robbery, with each device

This publication is produced to provide general information on the topic presented. It is distributed with the understanding that the publisher (Daigle Law Group, LLC) is not engaged in rendering legal or professional services. Although this publication is prepared by professionals, it should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

identified by a unique numerical code. At step one in this case, Google first provided 209 location data points from 19 accounts that appeared within the geofence during the hour-long period. Second, law enforcement narrows the list of devices and accounts and sends it back to Google. Google shares additional anonymized location data for the selected devices, covering one hour before to one hour after the robbery. This data is not restricted to the geofence. Here, Detective Hylton then requested Step Two information from nine accounts identified at Step One. Google responded by producing 680 data points from these accounts over the two-hour period. Finally, at Step Three, law enforcement would again attempt to shorten the list, and Google would provide the username and other identifying information for the requested accounts. At the last step, Detective Hylton requested the subscriber information for three accounts, which Google provided. One of these accounts belonged to the defendant, Chatrie.

A continued investigation into the defendant resulted in him being charged with the robbery. Hearing the case at the outset, the trial court denied Chatrie's motion to suppress the geofence evidence but acknowledged the serious privacy concerns these novel warrants raise. Opting to sidestep the question of whether the evidence obtained from the geofence warrant violated the Fourth Amendment, the court allowed the evidence to come in, justified under the good-faith exception to the exclusionary rule.[3] Chatrie appealed to the Fourth Circuit, asking the Circuit to hold that the geofence warrant violated his Fourth Amendment rights, requiring the fruits of the warrant to be suppressed.

On appeal, the Fourth Circuit affirmed the district court's denial of Chatrie's motion to suppress but offered a different reasoning than the rationale provided by the district court. While the lower court relied on the good-faith exception to the exclusionary rule, on appeal, the Fourth Circuit Court found that Chatrie did not have a reasonable expectation of privacy in the two hours of Location History data he voluntarily shared with Google. As a result, the Circuit held that the government's acquisition of this data from Google did not constitute a Fourth Amendment search.

Chatrie's appeal hinged on three key arguments. First, that the government conducted a Fourth Amendment search because law enforcement invaded his reasonable expectation of privacy by accessing his location history data. Second, he challenged the validity of the geofence warrant used to authorize the search, arguing that the warrant lacked probable cause and particularity. Third, that the good-faith exception to the exclusionary rule shouldn't apply to the warrant used in his case. The court rejected his reliance on *Carpenter*, citing the two rationales that justify applying the third-party doctrine: (1) the limited degree to which the information sought implicates privacy concerns, and (2) the voluntary exposure of that information to third parties.?

Tackling the first rationale: In this case, the nature of the information obtained, being two hours' worth of Chatrie's location history, is distinguishable from the revealing, long-term surveillance data obtained in cases like *Beautiful Struggle*, *Jones*, and *Carpenter*.? Instead, Chatrie's information was comparable to the type sought in *United States v. Knotts*—data that revealed short-term, public movements voluntarily conveyed to anyone who wanted to look.? In *Knotts*, the Court held that police single-use of a "beeper" to maintain its view on a vehicle they were following did not constitute a search. Moving to the second rationale: the Court found that Chatrie voluntarily exposed his location information to Google by taking the affirmative step of opting into Location History services, where two-thirds of Google's other users elected to decline this service.

This publication is produced to provide general information on the topic presented. It is distributed with the understanding that the publisher (Daigle Law Group, LLC) is not engaged in rendering legal or professional services. Although this publication is prepared by professionals, it should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

Finding that both rationales apply here, the Circuit found that the third-party doctrine governs this case. The government only accessed two hours of Chatrie's location data, which was not enough to reveal intimate details about his life. Chatrie had opted into Location History on July 9, 2018, meaning he knowingly and voluntarily allowed Google to collect and store his location information. The Court explained that by doing so, he accepted the risk that Google might share this information with the government. As a result, he cannot now argue that he had a reasonable expectation of privacy over this data, meaning that the government's attainment of the information did not constitute a Fourth Amendment search.

Law enforcement should closely monitor the Fourth Circuit's forthcoming en banc opinion in this case, as it is likely to provide significant clarification on the issues at hand and shape future interpretations of the law.

Take the next step in your professional development

Join Path of the Guardian today and gain 12 months of access to weekly training videos. Stay informed with concise, ten-minute sessions that tackle current policy and police practice issues. Plus, earn a certificate of completion to showcase your commitment to excellence.

Enroll now to stay ahead and make a lasting impact in your community!

Citations:

1. *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2024).
2. *United States v. Chatrie*, No. 22-4489, 2024 U.S. App. LEXIS 27770 (4th Cir. Nov. 1, 2024).
3. *United States v. Leon*, 468 U.S 897 (1984).
4. *Carpenter v. United States*, 585 U.S. 296.
5. *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc)
6. *United States v. Knotts*, 460 U.S. 276, 277, 281 (1983).

Date Created
01/07/2025

This publication is produced to provide general information on the topic presented. It is distributed with the understanding that the publisher (Daigle Law Group, LLC) is not engaged in rendering legal or professional services. Although this publication is prepared by professionals, it should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.