APPENDIX

United States Court of Appeals for the Fifth Circuit

No. 23-60321

United States Court of Appeals
Fifth Circuit
FILED
August 9, 2024
Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff—Appellee,

versus

JAMARR SMITH; THOMAS IROKO AYODELE; GILBERT MCTHUNEL, II,

Defendants—Appellants.

Appeal from the United States District Court
for the Northern District of Mississippi
USDC No. 3:21-CR-107-1

Before KING, HO, and ENGELHARDT, *Circuit Judges*.

KING, *Circuit Judge*:

A jury found Appellants guilty of robbery and conspiracy to commit robbery based on evidence obtained through a geofence warrant. On appeal, Appellants challenge the constitutionality of this novel type of warrant under the Fourth Amendment and maintain that the district court erred by failing to suppress all evidence derived therefrom.

We hold that the use of geofence warrants—at least as described herein—is unconstitutional under the Fourth Amendment. In doing so, we part ways with our esteemed colleagues on the Fourth Circuit. *See United*

States v. Chatrie, 107 F.4th 319 (4th Cir. 2024). With that said, we agree with the district court that, here, law enforcement acted in good faith in relying on this type of warrant. Accordingly, we AFFIRM the district court's denial of Appellants' motion to suppress.

I. Factual & Procedural Background

A. Underlying Offense

On February 5, 2018, three individuals acting in concert robbed Sylvester Cobbs, a Contract Route Driver with the United States Postal Service. As a Route Driver, Cobbs delivered and picked up mail from five rural post offices in DeSoto County and Tunica County, Mississippi. At the time of the robbery, Cobbs was headed to Lake Cormorant, the fourth of five stops he would make along his route.

The mail that Cobbs collected included registered mail bags, which contained cash receipts collected by the Postal Service from the sale of items such as money orders and stamps. By the time that Cobbs arrived at Lake Cormorant, he had already collected registered mail bags from three other post offices along his route.

At approximately 5:20 p.m., Cobbs arrived at the Lake Cormorant Post Office. As he normally would, Cobbs backed his mail truck up to the back door, where he would retrieve mail bags waiting for him inside the post office. Before Cobbs could open the back door to the post office, however, an unknown assailant—later determined to be Defendant-Appellant Gilbert McThunel—sprayed Cobbs with pepper spray, struck Cobbs multiple times with a handgun, threatened to kill him, and grabbed the registered mail bags from Cobbs's truck. The mail bags contained $60,706. Thereafter, the assailant fled, and Cobbs drove his truck to the front of the post office and called 911.

No suspect was arrested in connection to the robbery on the day of the occurrence. However, around three days after the robbery, Postal Inspector Stephen Mathews began his investigation and was able to locate a video of the incident taken from a camera located at a farm office across the street from the post office. The video showed a red Hyundai and a large white SUV in the area. The video revealed the assailant getting out of the SUV before the robbery, walking behind the building, and waiting for Cobbs to arrive. While behind the building, the assailant had his "hand up to his ear and elbow[] out" for multiple minutes, consistent with talking on a cell phone. However, the video does not show an actual cell phone. Later, after assaulting Cobbs, the assailant went back behind the building, squatted down, and began "looking at something in his hand" which appeared "indicative of" cell phone use. Although not visible on video, it is inferred that the suspect got back into the SUV before fleeing the scene. Based upon his examination of the video, Mathews surmised that three suspects were involved.

Sometime after obtaining the video footage, but prior to applying for any warrants, Mathews located a witness, Forrest Coffman, who lived across the street. Coffman had seen the red Hyundai "circling the area back and forth," and he decided to ask the driver if he was lost. The driver stated that he was looking for the highway. Coffman gave the driver directions, turned around, and went back inside his house. A "few moments later," Coffman heard a "bunch of commotion," stepped outside, and saw officers at the post office. Coffman walked over and spoke with law enforcement, where he described the person in the red Hyundai as a black male with a reddish color goatee. After meeting with law enforcement on the day of the incident, Coffman had no further involvement with the matter for approximately fifteen months.

By November 2018, nine months after the robbery, the Postal Inspection Service had not been able to identify any suspects from video

footage or witness interviews, and Postal Inspector Todd Matney testified that they "were having a problem identifying the individuals." However, during the course of their investigation, Matney and Mathews learned about "a new type of search warrant"—a "geofence warrant"—designed to "identify who might be present at the scene of a robbery." Believing that this warrant could help them rekindle their investigation, on November 8, 2018, Matney and Mathews applied for a geofence warrant seeking information from Google to locate potential suspects and witnesses in connection to the robbery.

B. Geofence Warrants: A Primer

As a relic of their novelty, "[t]here is a relative dearth of case law addressing geofence warrants." *United States v. Chatrie*, 590 F. Supp. 3d 901, 906 (E.D. Va. 2022) [hereinafter *Chatrie (Dist.)*]. As such, we provide a brief history of geofence warrants, as well as a description of law enforcement's process for obtaining them.[1]

Google received its first geofence warrant request in 2016.[2] *Id.* at 914; *United States v. Chatrie*, 107 F.4th 319, 323 (4th Cir. 2024) [hereinafter

---

[1] Congress has not yet taken a stance on law enforcement's use of geofence warrants. However, members have expressed their marked disapproval. In July 2020, Alphabet (Google's parent company) CEO Sundar Pichai appeared before the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law. *See* C-SPAN, *CEOs Mark Zuckerberg, Tim Cook, Jeff Bezos & Sundar Pichai Testify Before House Judiciary Cmte*, YouTube (July 29, 2020), https://perma.cc/7K5T-ACHJ (discussion at 1:45:17-1:47:50). During the hearing, Representative Kelly Armstrong called geofence warrants "the single most important issue" before the Subcommittee and contended that geofence warrants violate the Fourth Amendment. *Id.* In particular, Representative Armstrong believed that "people would be terrified to know that law enforcement can grab general warrants and get everybody's information anywhere." *Id.*

[2] Companies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrant requests, but Google is the most common recipient and "the only one known to

Chatrie (App.)]. Since then, requests for geofence warrants have "skyrocketed in number." *Chatrie (App.)*, 107 F.4th at 323–24. From 2017 to 2018 alone, requests to Google for geofence warrants increased over 1,500%. *Id.*; Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 834 (2022). In 2019, Google was receiving about 180 geofence warrant requests per week from law enforcement around the country, amounting to about 9,000 geofence requests for that year. Owsley, *Best Offense*, *supra* at 834; *Chatrie (Dist.)*, 590 F. Supp. 3d at 914. By 2020, that number went up to 11,500 geofence warrant requests. Owsley, *Best Offense*, *supra* at 834. By 2021, geofence warrants comprised more than 25% of all warrant requests Google received in the United States. *See* GOOGLE, SUPPLEMENTAL INFORMATION ON GEOFENCE WARRANTS IN THE UNITED STATES 1, https://perma.cc/XEU3-KEXJ; Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385, 389 & n.11 (2022). Moreover, the use of these warrants has not been limited to egregious or violent crimes. Law enforcement officials have obtained geofence warrants for investigations into stolen pickup trucks and smashed car windows. Amster & Diehl, *Against Geofences*, *supra* at 396; *see also In re Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20 M 297, 2020 WL 5491763, at *8 (N.D. Ill. July 8, 2020) ("The government's undisciplined and overuse of this investigative technique in run-of-the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials.").

"Unlike a warrant authorizing surveillance of a known suspect, geofencing is a technique law enforcement has increasingly utilized when the

---

respond." Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512–13 (2021).

crime location is known but the identities of suspects [are] not." *United States v. Rhine*, 652 F. Supp. 3d 38, 66 (D.D.C. 2023). Thus, geofence warrants effectively "work in reverse" from traditional search warrants. Amster & Diehl, *Against Geofences*, *supra* at 388 (internal quotation omitted). In requesting a geofence warrant, "[l]aw enforcement simply specifies a location and period of time, and, after judicial approval, companies conduct sweeping searches of their location databases and provide a list of cell phones and affiliated users found at or near a specific area during a given timeframe, both defined by law enforcement." *Geofence Warrants and the Fourth Amendment*, *supra* at 2509.

So far, Google has been the primary recipient of geofence warrants, in large part due to its extensive Location History database, known as the "Sensorvault."[3] Amster & Diehl, *Against Geofences*, *supra* at 389. Google

---

[3] In December 2023, Google authored a blog post where it announced its intent to modify how and where it stores Location History data. *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE: THE KEYWORD (Dec. 12, 2023), https://perma.cc/DN4Z-7CTA; *see also* Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants that Give Police Access to Location Data*, FORBES (Dec. 14, 2023, 5:43 PM EST), https://perma.cc/WM83-DAXM. Google's decision should make it "impossible for the company to access" Location History data in a move made "explicitly [to] bring an end to . . . dragnet location searches." Farivar & Brester, *Google Just Killed Warrants that Give Police Access to Location Data*, *supra*. In other words, these changes, in theory, "will eventually render the company unable to fulfill geofence warrants." Prathi Chowdri, *Emerging Tech and Law Enforcement: What Are Geofences and How Do They Work?*, LEXIPOL (Jan. 4, 2024) (internal quotation omitted), https://perma.cc/DNL3-XC56.

However, Google has not fully implemented its new storage methods; the migration will only be complete within "the next several months." *See* Stan Kaminsky, *Google Location History Is Now Stored Offline . . . Or Maybe Not*, KASPERSKY DAILY (Mar. 1, 2024), https://perma.cc/ZM6X-92JZ. In fact, the Government concedes that it "is still seeking Google geofences," and that even after Google changes its storage techniques, "the United States . . . may in the future seek geofence warrants from sources other than Google." Regardless, these facts do not affect this court's Fourth Amendment analysis regarding the constitutionality of the practice itself.

collects data from accounts of users who opt in to Google's Location History service. Location History is disabled by default. *Chatrie (App.)*, 107 F.4th at 322. For Location History to collect data, a user must make sure that the device-location setting is activated, and that Location Reporting is enabled. This is not to say, however, that enabling Location Reporting is a difficult task. Users are often asked to opt in to Location History "multiple times across multiple apps." *Id.* at 358 n.9 (Wynn, J., dissenting) (quoting *Chatrie (Dist.)*, 590 F. Supp. 3d at 908–09). In fact, "manually deactivating all [Location History] sharing remains difficult and discouraged." Amster & Diehl, *Against Geofences*, *supra* at 396–97 ("In 2018, an internal Google email explained that '[t]he current [user interface] *feels* like it is designed to make [limiting Location History collection] possible, yet [it is] difficult enough that people won't figure it out.'" (internal citation omitted)); *see also In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 737 n.3 (N.D. Ill. 2020) ("Published reports have indicated that many Google services on Android and Apple devices store the device users' location data even if the users seek to opt out of being tracked by activating a privacy setting that says it will prevent Google from storing the location data.").

Google's Android cell phones, which "comprise about 74% of the total number of smartphones worldwide," "automatically have an Android operating system, as well as various Google apps that could potentially store a user's location." Owsley, *Best Offense*, *supra* at 834. Apple, which makes approximately 23% of the world's smartphones, does not keep location data associated with its phones, but its phones still "often have various apps that . . . provide Google with a specific device's location." *Id.* at 834–35. In October 2018, Google estimated that approximately 592 million—or roughly one-third—of Google's users had Location History enabled.

Once a person enables Location History, Google begins to "log[] [the] device's location [into the Sensorvault], on average, every two minutes" by

"track[ing] [the] user's location across every *app* and every *device* associated with the user's account." *Chatrie (Dist.)*, 590 F. Supp. 3d at 908–09; *see also Chatrie (App.)*, 107 F.4th at 323 n.6. In other words, "'[o]nce a user opts into Location History, Google is always collecting data and storing *all* of that data' in the Sensorvault." *Rhine*, 652 F. Supp. 3d at 67 (quoting *Chatrie (Dist.)*, 590 F. Supp. 3d at 909). Location History is stored within the Sensorvault for at least eighteen months, but users may also request that the information be deleted themselves. Amster & Diehl, *Against Geofences*, *supra* at 394; *Rhine*, 652 F. Supp. 3d at 67.

Moreover, not only is the *volume* of data comprehensive, so is the *quality*. "Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *Chatrie (App.)*, 107 F.4th at 349 (Wynn, J., dissenting) (quoting *Chatrie (Dist.)*, 590 F. Supp. 3d at 907). The data is "considerably more precise than other kinds of location data, including cell-site location information because [Location History] is determined based on multiple inputs, including GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, and cell towers." *Rhine*, 652 F. Supp. 3d at 67 (internal quotations omitted). Google refers collectively to this data, regardless of its source, as "Location History." Amster & Diehl, *Against Geofences*, *supra* at 394. Location History data allows Google to "potentially locate an individual within about sixty feet or less," and in certain circumstances, down to three meters. Owsley, *Best Offense*, *supra* at 835; *Chatrie (Dist.)*, 590 F. Supp. 3d at 909. In fact, Location History data can "even discern elevation, locating the specific *floor in a building* where a person might be." *Chatrie (App.)*, 107 F.4th at 349 (Wynn, J., dissenting); *see also Chatrie (Dist.)*, 590 F. Supp. 3d at 908 (noting that Location History data can "determine if you are on the second [or first] floor of [a] mall"). However, Location History cannot estimate a device's location with absolute precision. Instead, when Google reports a

device's location, it includes both the source from which the specific datapoint was derived, and a "confidence interval" indicating Google's confidence in that estimated location. The smaller the radius, the more confident Google is in that phone's exact location. According to Google, it "aims to accurately capture roughly 68 percent of users within [its] confidence intervals." *Chatrie (Dist.)*, 590 F. Supp. 3d at 909 (internal quotation omitted); *Chatrie (App.)*, 107 F.4th at 323. "[I]n other words, there [is] a 68 percent likelihood that a user is somewhere inside the confidence interval." *Chatrie (Dist.)*, 590 F. Supp. 3d at 909 (internal quotation omitted); *Chatrie (App.)*, 107 F.4th at 323.

Using the raw data that it collects, Google builds "aggregate models" using a "proprietary, and therefore un-reviewed, algorithm" that transforms the data to assist with improving Google's services, including, for example, "decision-making in Google Maps." *Wells v. State*, 675 S.W.3d 814, 830 (Tex. App.—Dallas 2023, pet. granted); *Chatrie (Dist.)*, 590 F. Supp. 3d at 908; *Chatrie (App.)*, 107 F.4th at 323. It also uses the data to analyze "[its] customers[']... travel patterns, their history patterns, to make recommendations and sell advertising." In short, Google does not store this data for the purpose of law enforcement, but rather for commercial purposes. *Wells*, 675 S.W.3d at 830.

But, if you build it, they will come. *See Geofence Warrants and the Fourth Amendment*, *supra* at 2508. Early on, when law enforcement officials first started requesting geofence warrants, they would simply ask Google to identify all users who were in a geographic area during a given time frame. However, Google began taking issue with these early warrants, believing them to be a "potential threat to user privacy." *Chatrie (App.)*, 107 F.4th at 324. Thus, Google developed an internal procedure on how to respond to geofence warrants. *Id.* This procedure is divided into three steps.

Step 1

At Step 1, law enforcement provides Google with the geographical and temporal parameters around the time and place where the alleged crime occurred. Following, Google searches its Sensorvault for all users who had Location History enabled during the law enforcement-provided timeframe. *Chatrie (Dist.)*, 590 F. Supp. 3d at 914–15. Google is not capable of storing data in a way that enables it to search a specific area, nor does Google know which users have saved their Location History prior to its search. *Id.* at 915. Thus, for every single geofence warrant Google responds to, it must search each account in its entire Sensorvault—all 592 million—to find responsive user records. It cannot just look at individual accounts. *See Chatrie (App.)*, 107 F.4th at 324 ("Google does not keep any lists like this on-hand. So it must first comb through its entire Location History repository to identify users who were present in the geofence.").

After Google searches its Sensorvault, it determines which accounts were within the geographic parameters of the warrant and lists each of those accounts with an anonymized device ID. Google also includes the date and time, the latitude and longitude, the geolocation source used, and the map display radius (*i.e.*, the confidence interval). The volume of geofence data produced "depends on the size and nature of the geographic area and length of time covered by the geofence request." *Chatrie (Dist.)*, 590 F. Supp. 3d at 915. "Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data." *Id.* Rather, a Google Legal Investigation Specialist employee reviews the geofence warrant, consults with legal counsel, and works with law enforcement to assuage any of Google's concerns before turning the data over and moving on to Step 2. *Id.* at 907, 915–16; *see also Chatrie (App.)*, 107 F.4th at 324.

Step 2

At Step 2, law enforcement contextualizes and narrows the data. During this step, law enforcement reviews the anonymized list provided by Google and determines which IDs are relevant. As part of this review, "[i]f law enforcement needs additional de-identified location information for a certain device to determine whether that device is actually relevant to the investigation, law enforcement . . . can compel Google to provide additional . . . location coordinates *beyond* the time and geographic scope of the original request." *Chatrie (Dist.)*, 590 F. Supp. 3d at 916 (cleaned up); *Chatrie (App.)*, 107 F.4th at 324. The purpose of this additional data is to assist law enforcement in eliminating devices that are, for example, "not in the target location for enough time to be of interest, [or] were moving through the target location in a manner inconsistent with other evidence." *Chatrie (Dist.)*, 590 F. Supp. 3d at 916. As a general matter, "Google imposes no geographical limits on this Step 2 data." *Id.* (internal quotation omitted); *Chatrie (App.)*, 107 F.4th at 324. "Google does, however, typically require law enforcement to narrow the number of users for which it requests Step 2 data so that the Government cannot . . . simply seek geographically unrestricted data for *all* users within the geofence." *Chatrie (Dist.)*, 590 F. Supp. 3d at 916; *Chatrie (App.)*, 107 F.4th at 324.

Step 3

Finally, at Step 3, law enforcement compels Google to provide account-identifying information for the users that they determine are "relevant to the investigation." *Chatrie (App.)*, 107 F.4th at 324. This identifying information includes the names and emails associated with the listed device IDs. Using this information, law enforcement can then pursue further investigative techniques, such as cell phone tracking, or sending out additional warrants tailored to the specific information received.

* * *

As a final note, even given the vast amount of data Google has, and the unprecedented precision of Google's Location History, the results are not always spectacular. First, "[m]any geofence warrants do not lead to arrests." *Geofence Warrants and the Fourth Amendment*, *supra* at 2520. Moreover, "[m]any are rendered useless due to Google's slow response time, which can take as long as six months because of the Sensorvault's size and the large number of warrants that Google receives." *Id.* Second, as to warrants that are issued, the data Google returns is not always perfect, and sometimes contains false positives. In fact, there are already documented accounts of innocent bystanders being swept into geofence warrants based solely on their proximity to a crime.[4] In short, while false negatives appear to be "more extremely rare"—given the accuracy of Google's data—false positives are still an area of concern.

C. Geofence Application and Warrant at Issue

Returning to the matter at hand, the warrant here, like any other warrant, began with an Application for a Search Warrant. That application contained an attached affidavit from Matney, which Mathews helped write.

---

[4] For example, Zachary McCoy, an avid bike rider, was swept into a geofence search because on the day of a burglary, he biked past the victim's house three times within an hour. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020, 5:22 AM CST), https://perma.cc/9WJK-67TW. In another case, based on a Google geofence warrant, Arizona police officers jailed Jorge Molina for six days on suspicion of murder. Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020), https://perma.cc/GLJ8-AHP9. As it turns out, Molina's stepfather—the man ultimately arrested for the murder—had been using one of Molina's old cell phones, which inadvertently remained logged in to Molina's email and social media accounts. *Id.* As a result, Molina lost his job, was unable to pass a background check, and even lost title to his vehicle because police impounded his car during the investigation. *Id.*

Because this type of warrant was new, particularly to Mathews, the Postal Inspectors consulted with other law enforcement agencies when writing the application. Additionally, the Inspectors used several different "go-bys"—or form documents—to ensure that their application had all the necessary "technical language." Finally, the Inspectors also consulted with the U.S. Attorney's Office prior to seeking their warrant.

The affidavit stated that "there is probable cause to believe that the Google accounts identified in Section I of Attachment A, associated with a particular specified location at a particular specified time, contain evidence, fruits and instrumentalities of a violation of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee." However, as with any geofence warrant, no specific Google accounts were identified in Section I of Attachment A; rather, the Attachment only specified specific coordinates around the Lake Cormorant Post Office. The box created by those coordinates covered approximately 98,192 square meters.

The affidavit also provided a specific Probable Cause Statement. In that statement, the Inspectors detailed the two vehicles implicated in the robbery, Cobbs's description of the assailant, and a statement that, through a review of the video surveillance footage, "it appears the robbery suspect [was] possibly using a cellular device both before and after the robbery occur[ed]." Finally, the Inspectors included language in the application stating, in regard to Step 2 outlined above, that law enforcement "will seek any additional information regarding [relevant] devices through further legal process."

The application and affidavit were submitted to a U.S. magistrate judge, who issued the warrant on November 8, 2018. The language of the warrant largely tracked Google's three-step process outlined above:

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.

1. *Location information*. All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, **between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018;**

2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.

3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine the path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual

> location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)
>
> 4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

In summary, as to Step 1, the warrant authorized an hour-long search from 5:00 p.m. to 6:00 p.m. on February 5, 2018, within a geofence covering approximately 98,192 square meters around the Lake Cormorant Post Office. As to Step 2, the warrant authorized law enforcement to obtain additional Location History for a registered device identified as relevant within "60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset." However, prior to reaching Step 2, law enforcement was required to conduct "further legal process."

Google returned the Step 1 data in April 2019. Notably, Google's search was much broader than that specifically sought by the warrant, producing data from a circular area that was approximately 378,278 square meters, not 98,192 square meters. The search of Google's 592 million

accounts returned three anonymous device IDs within the requested parameters:

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radium (m)
1091610859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091610859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091610859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091610859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091610859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

Inspector Matney testified that after receiving this data, he reviewed the devices to ensure that they fell within the geofence coordinates.

However, prior to submitting Step 2, neither Matney nor Mathews applied for another warrant. Instead, Matney and Mathews decided themselves which device IDs were relevant and requested additional de-anonymized information for all three devices. The Inspectors determined that all three devices were relevant to their Step 2 inquiry because devices 1091610859 and 1577088768 registered multiple times within the geofence, and the third device—1353630479—could have been a potential witness. The Step 2 request was placed in May 2019, and the expanded information was received on May 30. However, no new devices were added through the information gained at Step 2.

Again, without seeking any new warrants, Matney and Mathews sent off their Step 3 request for all three devices on June 7, 2019. They received the de-anonymized information from Google on June 10, 2019. The following files were returned:

- 2165781.Key.cvs
- bleek2004.AccountInfo.txt
- jamarrsmith33.AcountInfo.txt
- permanentwavesrecords.AccountInfo.txt

Through these files, Mathews was able to determine that "jamarrsmith33.AcountInfo.txt" was Jamarr Smith's email account and "bleek2004.AcountInfo.txt" was Gilbert McThunel's email account. The third email account associated with "permanentwavesrecords.AccountInfo.txt" was deemed irrelevant to the investigation.

Now, no longer devoid of leads, Mathews and Matney took "[a] bunch of investigative steps" related to Smith and McThunel, including sending additional non-geofence warrants to Google regarding Smith and McThunel's Google accounts, accessing their CLEAR database profiles, investigating cell tower data related to Smith and McThunel, and sending non-geofence warrants to phone companies for Smith and McThunel's account information. These additional steps revealed multiple phone calls between Smith and McThunel during the time of the robbery, and allowed for further geolocation of Appellants using historical cell phone record analysis.

Additionally, through a search of Smith's phone records and his friends on Facebook, the Inspectors were able to identify Thomas Iroko Ayodele as a suspect. Finally, on July 1, 2019, Postal Inspector Dwayne Martin reapproached witness Forrest Coffman and asked him to participate in a photo lineup. Although Coffman was unable to identify McThunel or Ayodele in their respective lines, Coffman did identify Smith as the person he saw driving the red Hyundai. In sum, all evidence connecting Appellants to this crime was derived from information obtained from Google pursuant to the geofence warrant.

D. Pretrial & Trial Posture

The Government initiated the instant action by issuing an indictment on October 27, 2021. Count I of the indictment alleged that Appellants had a conspiracy to rob the Lake Cormorant Post Office, and Count II alleged the

actual robbery. On November 4, 2022, Smith filed a Motion to Suppress—which the other Appellants joined—seeking to suppress all evidence derived from the November 2018 geofence warrant which was used to identify them as suspects.

Appellants raised multiple arguments related to the constitutionality of the geofence warrant. First, Appellants contended that they had a reasonable expectation of privacy in their Google Location History data, and that this geofence warrant violated that privacy interest as a categorically unconstitutional general warrant. Second, Appellants argued that the specific warrant at issue was invalid from its inception because it lacked probable cause and particularity. Third, Appellants argued that even if the warrant was valid, the Government did not undertake "further legal process" to obtain additional information from Google as required by the warrant, making Step 2 and Step 3 of the search warrantless and illegal. Finally, Appellants maintained that the good-faith exception set forth in *United States v. Leon*, 468 U.S. 897 (1984), did not excuse the defects of the warrant, especially in light of the fact that the affidavit in support of the warrant contained a knowing and intentionally false statement—specifically, that "it appear[ed] the robbery suspect [was] possibly using a cellular device both before and after the robbery occur[ed]"—making the warrant invalid pursuant to *Franks v. Delaware*, 438 U.S. 154, 164–65 (1978). As such, Appellants concluded, the exclusionary rule should apply, and all the evidence seized should be suppressed as fruit of the poisonous tree.

On January 31, 2023, the district court conducted a hearing on Appellants' Motion to Suppress. At the hearing, the Government called its two Investigators, Matney and Mathews, and Appellants called an expert, Spencer McInvaille. In relevant part, Matney and Mathews testified as to: their unfamiliarity with geofence warrants; the steps they took to request a geofence warrant and receive information from Google; their consultation

with the U.S. Attorney's Office; their review of surveillance footage purporting to show the robbery suspect acting consistently with cell phone usage (*e.g.*, holding his hand up to his ear); and their understanding that the language in the warrant requiring "further legal process" at Steps 2 and 3 meant the process of law enforcement "demand[ing]" information from Google, not the process of law enforcement seeking any additional warrants from the court.

McInvaille provided expert testimony to the court about digital forensics and geolocation analysis, including, in relevant part, Google Location History data. McInvaille explained to the district court that warrants submitted to Google are typically used to seek information about suspects when law enforcement knows the suspect has a Google account. In contrast, law enforcement utilizes geofence warrants and Google Location History when they do not have any leads, but nevertheless want to search through Google's data (*i.e.*, the Sensorvault) to find suspects. McInvaille outlined the three-step geofence warrant process described *supra*, and explained that as part of that process, Google is required to search every Google account with Location History enabled. Finally, McInvaille testified that, given his experience in other cases, the language requiring "further legal process" in this warrant would have required additional warrants at each step of the geofence process.

On February 10, 2023, after considering the parties' briefing and the evidence presented at the hearing, the district court denied Appellants' motion to suppress. Trial commenced on February 21, 2023. After a four-day trial, the jury returned a guilty verdict against all three Appellants as to both counts. Appellants were sentenced on June 13, 2023, to prison terms ranging from 121 to 136 months. Following, Appellants filed a Motion for New Trial and Motion for Judgment of Acquittal. The district court denied the motion. Appellants timely appealed.

II. Standard of Review

"When reviewing the denial of a motion to suppress evidence, this court reviews the district court's factual findings for clear error and the district court's conclusions regarding the sufficiency of the warrant and the constitutionality of law enforcement action de novo." *United States v. Perez*, 484 F.3d 735, 739 (5th Cir. 2007). We view the evidence in the light most favorable to the prevailing party below—here, the Government. *See United States v. Pack*, 612 F.3d 341, 347 (5th Cir. 2010).

III. Analysis

The Fourth Amendment guarantees individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend IV. The "basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter v. United States*, 585 U.S. 296, 303 (2018) (quoting *Camara v. Mun. Ct. of City and Cnty. of S.F.*, 387 U.S. 523, 528 (1967)). Moreover, the Supreme Court has established that "the Fourth Amendment protects people, not places," and the Court has "expanded [its] conception of the Amendment to protect certain expectations of privacy as well." *Id.* at 304 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Court] ha[s] held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Evidence seized in violation of the Constitution is subject to suppression. *See Hudson v. Michigan*, 547 U.S. 586, 590 (2006).

A. Reasonable Expectation of Privacy

The threshold question posed by this case is whether geofencing is a search under the Fourth Amendment. "A Fourth Amendment privacy interest is infringed when the government physically intrudes on a constitutionally protected area or when the government violates a person's 'reasonable expectation of privacy.'" *United States v. Turner*, 839 F.3d 429, 434 (5th Cir. 2016) (quoting *United States v. Jones*, 565 U.S. 400, 406 (2012)). To assess whether a "reasonable expectation of privacy" exists, the Supreme Court has applied Justice Harlan's two-fold approach as explained in his concurrence in *Katz v. United States*, 389 U.S. 347. *See Jones*, 565 U.S. at 406. Specifically, for Fourth Amendment protections to attach to a person's privacy interest, the person first must "have exhibited an actual (subjective) expectation of privacy." *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Second, that expectation must "be one that society is prepared to recognize as 'reasonable.'" *Id.* (Harlan, J., concurring).

Smith and McThunel contend that they have a reasonable expectation of privacy in their respective location information retrieved in response to a geofence warrant.[5] This argument is rooted in the application of *Carpenter v.*

---

[5] Ayodele also attempts to join Smith and McThunel's arguments. However, as noted above, Ayodele's information was never retrieved in response to a geofence warrant—his involvement in this robbery was deduced through a search of Smith's phone records and Smith's friends on Facebook performed after the geofence search. As such, Ayodele may lack Fourth Amendment standing to join Smith and McThunel because even if he has an expectation of privacy in his own Google Location History data, he may not have an expectation of privacy in the Google Location History data of an unrelated third-party. *See United States v. Davis*, No. 23-10184, 2024 WL 3573478, at *5–7 (11th Cir. 2024) (concluding that a defendant lacked Fourth Amendment standing to challenge a geofence warrant that produced his girlfriend's Google Location History data because "[e]ven if a person has a privacy interest in the data on his own phone, he does not have that interest in the data on someone else's phone.").

United States, 585 U.S. 296, arguably the most relevant Supreme Court precedent addressing law enforcement's investigatory use of cellular consumer data. *See* Amster & Diehl, *Against Geofences*, *supra* at 406. In *Carpenter*, prosecutors, without a warrant supported by probable cause, received from a criminal defendant's wireless carriers cell-site location information ("CSLI") that tracked the defendant's whereabouts over the course of several days.[6] 585 U.S. at 302. From this data, prosecutors were able to produce maps that placed the defendant's phone near four robberies. *Id.* at 302–03. The court of appeals affirmed the defendant's convictions, concluding that the defendant's privacy interest in CSLI was not entitled to Fourth Amendment protection because "cell phone users voluntarily convey cell-site data to their carriers as a means of establishing communication." *Id.* at 303 (internal quotation omitted).

The Supreme Court reversed. *Id.* at 321. As a starting point, the Court acknowledged that a majority of the Court had "already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Id.* at 310; *see Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). The Court then expressed

---

Regardless, we do not and need not answer this question today—as discussed further *infra*, Smith and McThunel *do* have Fourth Amendment standing to bring their respective constitutional challenges, and our ultimate disposition as to all three Appellants hinges on the good faith exception. *See Byrd v. United States*, 584 U.S. 395, 411 (2018) ("Because Fourth Amendment standing is subsumed under substantive Fourth Amendment doctrine, it is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.").

[6] As the Supreme Court in *Carpenter* explained, CSLI is the time-stamped record that is generated each time a phone connects to "cell sites," the network of radio antennas that provide signal to cell phones. 585 U.S. at 300–01.

concern with the government having unfettered access to CSLI, noting that this data provides "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). The Court further expressed concern that this precise, sensitive data could be accessed by the government "[w]ith just the click of a button." *Id.* And, in contrast to a GPS device attached to a person's car, a cell phone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 311–12. The Court concluded that the criminal defendant had a "reasonable expectation of privacy in the whole of his physical movements." *Id.* at 313.

The Court then addressed the third-party doctrine, which provides that generally, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 308 (quoting *Smith*, 442 U.S. at 743–44). The Court declined to apply the third-party doctrine to the collection of CSLI, notwithstanding the fact that this data is technically voluntarily provided from users to private wireless carriers. As the Court noted, there is a "world of difference between the limited types of personal information" addressed in the Court's prior third-party doctrine precedent "and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 314. Furthermore, the Court found the notion that users "voluntarily" provide this information to private entities dubious. Carrying a cell phone is "indispensable to participation in modern society," and, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.*

at 315. "As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." *Id.* (quoting *Smith*, 442 U.S. at 745).

Chief Justice Roberts's majority opinion in *Carpenter* speaks at length about the privacy interests inherent in location data, and it expresses grave concern with the government being able to comprehensively track a person's movement with relative ease due to the ubiquity of cell phone possession. The Court acknowledged "some basic guideposts" in resolving questions related to the Fourth Amendment's protections of privacy interests, including securing "the privacies of life against arbitrary power," and placing "obstacles in the way of a too permeating police surveillance." *Carpenter*, 585 U.S. at 305 (internal quotations omitted). The Court also recognized the necessity of applying the Fourth Amendment to systems of advanced technology, expressing concern that CSLI is approaching "GPS-level precision," with wireless carriers having the capability to "pinpoint a phone's location within 50 meters." *Id.* at 313; *see also Riley v. California*, 573 U.S. 373, 396 (2014) (acknowledging the privacy concerns implicated by cell phone location data that "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building").

Many of the concerns expressed by Chief Justice Roberts in his *Carpenter* opinion are highly salient in the context of geofence warrants. Perhaps the most alarming aspect of geofences is the potential for "permeating police surveillance." As Chief Justice Roberts explained, modern cell phones enable the government to achieve "near perfect surveillance"; carrying one of these devices is essentially a prerequisite to participation in modern society, and users "compulsively carry cell phones with them all the time." *Id.* at 311–12, 315. Geofences also exemplify the Court's concern with pinpoint location data—this technology provides more

precise location data than either CSLI or GPS. *Geofence Warrants and the Fourth Amendment*, *supra* at 2510. Furthermore, obtaining data through geofences, like obtaining data through CSLI, is "remarkably cheap, easy, and efficient compared to traditional investigative tools." *Carpenter*, 585 U.S. at 311. With "just the click of a button," the government can search the pinpoint locations of over half a billion people with Location History enabled. *See id.*

But while we see the parallels between CSLI and Location History data, our colleagues on the Fourth Circuit—the first federal Circuit to address whether geofencing is a "search" subject to the Fourth Amendment—saw Location History data differently. *See Chatrie (App.)*, 107 F.4th at 330. Characterizing Location History data as nothing more than a "record of a person's single, brief trip," the Fourth Circuit found that geofencing does not contravene a person's "reasonable expectation of privacy" because the data implicated by geofences is "far less revealing than that obtained in *Jones*[or] *Carpenter*." *Id.* at 330–31.[7] With great respect to our colleagues on the Fourth Circuit, we disagree. While it is true that geofences tend to be limited temporally, the potential intrusiveness of even a snapshot of precise location data should not be understated. As two commentators noted:

---

[7] In *United States v. Davis*, the Eleventh Circuit appeared to agree with the Fourth Circuit that geofence warrants "do[] not implicate the same privacy concerns raised in *Carpenter*." *See* 2024 WL 3573478, at *6. However, *Davis* ultimately concerned a defendant's Fourth Amendment standing to challenge a geofence warrant that obtained *his girlfriend's* Google Location History data, *not* his own data. *Id.* at *6. Thus, the Eleventh Circuit's discussion of the intrusiveness of Google Location History data ultimately does not appear to have been dispositive to its holding. *See id.* at *6–7 ("Because the geofence revealed the location of an open program that was not [the defendant's] and was not on a phone in his exclusive possession or control, he cannot argue that he had a privacy interest in this data that gives him Fourth Amendment standing to challenge the search.").

> [E]ven a brief snapshot can expose highly sensitive information—think a visit to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar," or a location other than home during a COVID-19 shelter-in-place order.

Amster & Diehl, *Against Geofences*, *supra* at 408 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Plus, such location tracking can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences. As another commentator described:

> Even a geofence warrant that limits itself to a single day could follow a person from the interior of their home, among the rooms of their dwelling, to the location of a crime, then to a place of worship, then perhaps to a new home, such as that of a relative or friend, and among the rooms of that second dwelling.

A. Reed McLeod, Note, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 WM. & MARY BILL RTS. J. 531, 549 (2021).[8] In short,

---

[8] The Fourth Circuit acknowledged and dismissed these considerations because, *inter alia*, the defendant—like the defendants in the case at bar—"d[id] not contend that the warrant revealed his own movements within his own constitutionally protected space," and thus the defendant lacked Fourth Amendment standing to challenge geofencing on those grounds. *See Chatrie (App.)*, 107 F.4th at 330 n.17, 337 n.26. We disagree—this conclusion directly conflicts with *Carpenter*.

In *Carpenter*, the Supreme Court's analysis of whether the government's access of the defendant's CSLI impeded his reasonable expectation of privacy was *not* based on a review of the specific results of the search in that case. *See generally* 585 U.S. at 309–13. Rather, the Supreme Court analyzed the *general capabilities* of CSLI, and asked whether the *ability* for CSLI "to chronicle a person's past movements through the record of his cell phone signals" created an expectation of privacy. *Id.* at 309. In other words, it did not matter whether *that* defendant *happened* to stay outside of a constitutionally protected area during a search or not. The question was whether the technology utilized by law

geofence location data is invasive for Fourth Amendment purposes. Of particular concern is the fact that a geofence will retroactively track anyone with Location History enabled, regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection.[9]

Moreover, *Carpenter*'s application to the third-party doctrine in this case is straightforward. As the Court in *Carpenter* explained, while cell phone data is held by private corporations, on a practical level, it is unreasonable to think of cell phone users as voluntarily assuming the risk of turning over

---

enforcement had the *capability* of providing data that offered "an all-encompassing record of [a person's] whereabouts," regardless of whether that person actually entered spaces that are traditionally considered protected under the Fourth Amendment. *Id.* at 311. And, when a person has a "reasonable expectation of privacy in the place or thing searched or seized," he or she has Fourth Amendment standing. *See United States v. Gaulden*, 73 F.4th 390, 392 (5th Cir. 2023).

Here, the analysis is no different. The question is whether Location History data has the capability of revealing intimate, private details about a person's life, thus conferring a "reasonable expectation of privacy." This is general inquiry, not a retroactive, *post-hoc* examination based on the *results* of the search in our case. A conclusion to the contrary would be enigmatic. *See Chatrie (App.)*, 107 F.4th at 351 (Wynn, J., dissenting) ("The government . . . cannot circumvent the Constitution merely because, by sheer luck, its target did not stray from the safe zone.").

[9] Some have argued that the privacy concerns presented by geofences are ameliorated by the fact that information sent to law enforcement is, at first, anonymized. *See, e.g.*, *In re Search of Info. Stored at Premises Controlled by Google*, No. 2:22-MJ-01325, 2023 WL 2236493, at *8 (S.D. Tex. Feb. 14, 2023). However, it is undisputed that the data is eventually de-anonymized. And, even setting that point aside, the effectiveness of data anonymization has been called into question by researchers, given that anonymous data can be cross-referenced to reveal identities. *See* Amster & Diehl, *Against Geofences*, *supra* at 409; *see also* Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. TIMES (Feb. 5, 2021), https://perma.cc/KMP3-3QSV (detailing journalists' efforts to identify individuals contained in anonymized datasets of smartphone locations); Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), https://perma.cc/L5DL-MPZM. Thus, we find this argument wanting.

comprehensive dossiers of their physical movements to third parties. *Carpenter*, 585 U.S. at 315. In a way, *Carpenter* acknowledged that, at least in some instances, the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Given the ubiquity—and necessity—in the digital age of entrusting corporations like Google, Microsoft, and Apple with highly sensitive information, the notion that users voluntarily relinquish their right to privacy and "assume[] the risk" of this information being divulged to law enforcement is dubious. *See Smith*, 442 U.S. at 745.

It is true that this case is slightly distinguishable from *Carpenter*; namely, that users opt in to having their Location History monitored. Indeed, this was the other consideration that persuaded the Fourth Circuit that geofencing is not a "search" subject to the Fourth Amendment. *See Chatrie (App.)*, 107 F.4th at 331–32. Again, with great respect, we are not convinced.

As anyone with a smartphone can attest, electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884–88 (2013). *See generally* Hannah J. Hutton & David A. Ellis, *Exploring User Motivations Behind iOS App Tracking Transparency Decisions*, PROC. OF THE 2023 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS., Apr. 2023, at 1, 7–8, 10 (detailing general "confusion" with, and "misconceptions" about, Apple's data-tracking opt-in prompts due, in part, to those prompts' "lack of clarity"). Google's Location History opt-in process is no different. As described above, users are bombarded multiple times with requests to opt in across multiple apps. *See Chatrie (Dist.)*, 590 F. Supp. 3d at 908–09. These requests typically innocuously promise app optimization, rather than reveal the fact that users' locations will be comprehensively stored in a "Sensorvault," providing

Google the means to access this data and share it with the government. *See Chatrie (App.)*, 107 F.4th at 359–60 (Wynn, J., dissenting); *see also* Defendant Okello Chatrie's Supplemental Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 15–17, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. May 22, 2020), 2020 WL 4551093, ECF No. 104. Even Google's own employees have indicated that deactivating Location History data based on Google's "limited and partially hidden" warnings is "difficult enough that people won't figure it out." *Chatrie (App.)*, 107 F.4th at 360, 367 (Wynn, J., dissenting) (quoting *Chatrie (Dist.)*, 590 F. Supp. 3d at 913, 936); Amster & Diehl, *Against Geofences*, *supra* at 396–97.

But you don't have to take our word for it—others have similarly questioned the "voluntary" nature of Google's opt-in process. *See, e.g.*, *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 737 & n.3 ("The Court finds it difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government's ability to obtain—easily, quickly and cheaply—their precise geographical location at virtually any point in the history of their use of the device."); McLeod, *Geolocating the Fourth Amendment*, *supra* at 543 ("[C]onsider a Google user's consent to Location History . . . . [u]sers either opt in with less than explicit notice given to them, or even with good notice, without a full realization of the potential consequences to their privacy if they opt in. Second, users may understand the notice they have been given, but misunderstand the accuracy of the movement patterns as expressed in the location data collected by tech companies."); *Chatrie (Dist.)*, 590 F. Supp. 3d at 935 (acknowledging that users take "some affirmative steps to enable location history," yet concluding that "those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day"); *see*

also Chatrie (App.), 107 F.4th at 356–61 (Wynn, J., dissenting); Amster & Diehl, *Against Geofences*, *supra* at 396–97, 409–10.

Not to mention, the fact that approximately 592 million people have "opted in" to comprehensive tracking of their locations itself calls into question the "voluntary" nature of this process. In short, "a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant, even if some text offered warning along the way." *Chatrie (Dist.)*, 590 F. Supp. 3d at 936.

* * *

To conclude, we hold that law enforcement in this case *did* conduct a search when it sought Location History data from Google. Given the intrusiveness and ubiquity of Location History data, Smith and McThunel correctly contend that they have a "reasonable expectation of privacy" in their respective data. Additionally, per *Carpenter*, the third-party doctrine does not apply.

B. General Constitutionality

Having concluded that the acquisition of Location History data via a geofence is a search, it follows that the government must generally obtain a warrant supported by probable cause and particularity before requesting such information. *Carpenter*, 585 U.S. at 316. Accordingly, we turn to the issue of whether geofence warrants satisfy this mandate, addressing Appellants' argument that these novel warrants resemble unconstitutional general warrants prohibited by the Fourth Amendment.[10]

---

[10] Because the Fourth Circuit concluded that law enforcement did not conduct a search when it sought Location History data from Google, it did not reach the question of

"[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403. "General warrants" are warrants that "specif[y] only an offense," leaving "to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981); *Geofence Warrants and the Fourth Amendment*, *supra* at 2518.

It is undeniable that general warrants are plainly unconstitutional. Indeed, "it would be a needless exercise in pedantry to review again the detailed history of the use of general warrants as instruments of oppression from the time of the Tudors, through the Star Chamber, the Long Parliament, the Restoration, and beyond." *Stanford v. Texas*, 379 U.S. 476, 482 (1965). Thus, courts have recognized that no warrant "can authorize the search of everything or everyone in sight." *Geofence Warrants and the Fourth Amendment*, *supra* at 2518; *cf. Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996) ("[A] warrant to search 'all persons present' for evidence of a crime may only be obtained when there is reason to believe that all those present will be participants in the suspected criminal activity."); *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) ("[A]n 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity.").

---

whether geofence warrants pass muster under the Fourth Amendment's warrant requirement.

When law enforcement submits a geofence warrant to Google, Step 1 forces the company to search through its *entire* database to provide a new dataset that is derived from its entire Sensorvault. In other words, law enforcement cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for *all* of their locations at a given point in time. Moreover, this search is occurring while law enforcement officials have *no idea* who they are looking for, or whether the search will even turn up a result. Indeed, the quintessential problem with these warrants is that they *never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search.[11] That is constitutionally insufficient.

Geofence warrants present the exact sort of "general, exploratory rummaging" that the Fourth Amendment was designed to prevent. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also Riley*, 573 U.S. at 403; *Geofence Warrants and the Fourth Amendment*, *supra* at 2519. In fact, Google Maps creator Brian McClendon has called these warrants "fishing expedition[s]," and explained that Google employees originally assumed law enforcement would only seek Location History data on specific people—a reality that did not come true. Jennifer Valentino-DeVries, *Tracking Phones,*

---

[11] As Professor Stephen Henderson explains in his discussion of CSLI, focusing probable cause on the group rather than the individual "would mean that a larger database is always preferred" by law enforcement, because "by definition there will be evidence of crime in that larger set." Stephen E. Henderson, Response, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. *See Also* 28, 40–41 (2016). Doing so leads to an "absurd" understanding of probable cause: "[A] prosecutor confident that *a* bank customer is committing tax fraud could access the combined records of *all* customers of that bank because, somewhere in there, she is very sure is evidence of crime." *Id.* at 41. Henderson argues, in the context of CSLI, it must be the case that probable cause is required for "each person's obtained records," meaning here "each phone number contained within the dump." *Id.* The same argument applies with full force to Google accounts containing Location History data.

Google Is a Dragnet for the Police, N.Y. TIMES (Apr. 13, 2019), https://perma.cc/NCF3-H5DP. "Awareness that the government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring.). And, when these core rights are at issue, the warrant requirement must "be accorded the most scrupulous exactitude." *See Stanford*, 379 U.S. at 485.

Here, the Government contends that geofence warrants are not general warrants because they are "limited to specified information directly tied to a particular [crime] at a particular place and time." This argument misses the mark. While the *results* of a geofence warrant may be narrowly tailored, the *search* itself is not. A general warrant cannot be saved simply by arguing that, after the search has been performed, the information received was narrowly tailored to the crime being investigated. These geofence warrants fail at Step 1—they allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found.[12]

---

[12] The Fourth Circuit—albeit in the context of determining whether law enforcement's acquisition of Location History data qualified as a "search" under the Fourth Amendment—appeared to contend that Google's search at Step 1 is irrelevant to our inquiry because *Google*, rather than *law enforcement*, conducts that search. *See Chatrie (App.)*, 107 F.4th at 330 n.16. Instead, the Fourth Circuit concluded that "the proper focus of our inquiry [should be] . . . the government's access of two hours' worth of [defendant's] Location History data," *i.e.*, Step 2, because "a search only occurs once the *government* accesses the requested information." *Id.*

This proposition is breathtaking. In essence, the Fourth Circuit appears to conclude that law enforcement may flaunt the Fourth Amendment by simply offloading their *act* of "searching" on to a third party, and waiting to see if that third party's search produces any fruit before applying for a warrant. Moreover, by implication, if the third party's search produces zero evidence, *law enforcement never conducted any search at all*.

But the Supreme Court has clearly stated that the Fourth Amendment protects against *both* searches *and* seizures "effected by a private party . . . if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S.

In sum, geofence warrants are "[e]mblematic of general warrants" and are "highly suspect per se." *Geofence Warrants and the Fourth Amendment*, *supra* at 2520; Amster & Diehl, *Against Geofences*, *supra* at 433–34; Chad Marlow & Jennifer Stisa Granick, *Celebrating an Important Victory in the Ongoing Fight Against Reverse Warrants*, ACLU (Jan. 29, 2024), https://perma.cc/SC2R-S7PJ ("The constitutionality of reverse warrants is highly suspect because, like general warrants that are prohibited by the Fourth Amendment, they permit searches of vast quantities of private, personal information without identifying any particular criminal suspects or demonstrating probable cause to believe evidence will be located in the corporate databases they search."); *Chatrie (App.)*, 107 F.4th at 353 (Wynn, J., dissenting) ("[A] [geofence] warrant is uncomfortably akin to the sort of 'reviled' general warrants used by English authorities that the Framers intended the Fourth Amendment to forbid.").

This court "cannot forgive the requirements of the Fourth Amendment in the name of law enforcement." *Berger v. New York*, 388 U.S. 41, 62 (1967). Accordingly, we hold that geofence warrants are general warrants categorically prohibited by the Fourth Amendment. We now move on to suppression and the good-faith exception to the warrant requirement.

C. Good-Faith Exception

In *United States v. Leon*, 468 U.S. 897, 913 (1984), the Supreme Court evaluated the Fourth Amendment exclusionary rule, and opined that

---

602, 613–14 (1989). And, here, all of Google's actions, including at Step 1, are "conducted in response to legal compulsion and 'with the participation or knowledge of [a] governmental official.'" *Geofence Warrants and the Fourth Amendment*, *supra* at 2516 (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). Accordingly, law enforcement must abide by the Fourth Amendment not only when Google provides them with a final list of names, but also when they instruct Google to search its entire Sensorvault to produce those names. *Id.* Put differently, the proper focus of our inquiry *does* include Step 1.

evidence seized by officers reasonably relying on a warrant issued by a detached and neutral magistrate judge should be admissible.[13] However, the Court articulated four circumstances where this "good faith" exception does not apply:

> (1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; (2) when the issuing magistrate wholly abandoned his judicial role; (3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and (4) when the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers cannot reasonably presume it to be valid.

United States v. Woerner, 709 F.3d 527, 533–34 (5th Cir. 2013) (citing *Leon*, 468 U.S. at 921–25).

Appellants argue that three of the *Leon* circumstances apply in this case. First, Appellants contend that Inspectors knowingly or recklessly included a false statement in the warrant affidavit, specifically, the statement that "it appear[ed] the robbery suspect [was] possibly using a cellular device

---

[13] Appellants argue that "[t]here is no such thing as relying on a general warrant in good-faith," and that an application of *Leon* is categorically unnecessary. Their argument is well taken, but we decline to adopt that stance today. Appellants point the court to *Groh v. Ramirez*, 540 U.S. 551, 558, 563 (2004), which held that "no reasonable officer could believe that a warrant that plainly did not comply with [the particularity] requirement was valid," and which cited *Leon* even though the issue in *Groh* was ultimately about qualified immunity. However, *Groh* did not involve a novel advancement in law enforcement technology—in fact, *Groh* involved an essentially run-of-the-mill warrant to search for guns in a house. *Id.* at 554–57. Given the novelty and complexity of geofence warrants, as well as the dearth of legal authority on the topic of geofence warrants to guide law enforcement, *Groh* is distinguishable on its facts. Moreover, the other cases cited by Appellants are also unavailing, as a majority were decided prior to *Leon*. Accordingly, we hold that *Leon* applies to our analysis.

both before and after the robbery occur[ed]." Appellants maintain that Matney and Mathew's use of a "go-by" is indicative of the fact that they had no idea whether a cell phone was used, and that this is "by definition reckless at best." We disagree. As the district court noted, video evidence of the assailant appears to show body language consistent with cell phone use. Mathews and Matney reviewed this video footage in addition to using a "go-by." In essence, Appellants ask this court to ignore Matney's testimony that the Inspectors based their probable cause statement in the warrant affidavit, in part, on this footage. Because this court is highly deferential to the district court's factfinding, and because the court reviews evidence in the light most favorable to the Government, *see Pack*, 612 F.3d at 347, Appellants' argument fails.

Appellants' second and third *Leon* arguments pertain to probable cause and particularity—*i.e.*, that the warrant was "completely devoid" of probable cause, or that it was "facially deficient" in particularity, rendering the Inspectors' conclusions unreasonable. Again, we disagree. Here, we find the rationale behind the Fourth Circuit's opinion in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), persuasive. In *McLamb*, the Fourth Circuit declined to suppress evidence when officers were utilizing "cutting edge investigative techniques" and consulted with attorneys from the Department of Justice. *Id.* at 690–91. Here, the Inspectors likewise had conversations with other law enforcement officials and the U.S. Attorney's Office prior to submitting their warrant. To this end, we, like the district court "struggle[] to see any wrongful conduct to deter," because "the conduct of law enforcement in this case seem[ed] reasonable and appropriate when considering the specific circumstances with which the investigators were faced."

At bottom, "but-for causality is only a necessary, not a sufficient, condition for suppression." *Hudson*, 547 U.S. at 592. This court must also

weigh the "substantial social costs" of exclusion against "deterrence benefits," the "existence of which [is also] a necessary condition for exclusion." *Id.* at 594–96 (internal quotations omitted). Here, the social costs of exclusion are admittedly considerable, including the consequences "that exclusion of relevant incriminating evidence always entails (viz., the risk of releasing dangerous criminals into society)." *Id.* at 595. Additionally, the deterrence benefits here are not clear. The Inspectors were utilizing a cutting-edge investigative technique with which neither Inspector had personal experience. To that end, the Inspectors diligently attempted to make sure that their warrant comported with the Fourth Amendment by communicating with other law enforcement agencies and the U.S. Attorney's Office, and the Inspectors exhibited no malicious intent through the actions that they took. Thus, we cannot fault law enforcement's actions considering the novelty of the technique and the dearth of court precedent to follow.[14] Accordingly, none of *Leon*'s circumstances apply, and the district court correctly declined to suppress evidence under the good-faith exception to the warrant requirement.[15]

---

[14] For the same reasons, we agree with the district court that the Inspectors' mistaken belief regarding the meaning of the phrase "further legal process," and their failure to apply for additional warrants at Steps 2 and 3, do not preclude the applicability of the good faith exception.

[15] Appellants also argue that the district court erred by failing to exclude the Government's expert witness, Christopher Moody, at trial as unreliable under *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). We disagree. "District courts enjoy wide latitude in determining the admissibility of expert testimony, and the discretion of the trial judge and his or her decision will not be disturbed on appeal unless manifestly erroneous." *Watkins v. Telsmith, Inc.*, 121 F.3d 984, 988 (5th Cir. 1997) (internal quotation omitted). "'Manifest error' is one that is 'plain and indisputable, and that amounts to a complete disregard of the controlling law.'" *Kim v. Am. Honda Motor Co.*, 86 F.4th 150, 159 (5th Cir. 2023) (quoting *Bear Ranch, L.L.C. v. Heartbrand Beef, Inc.*, 885 F.3d 794, 802 (5th Cir. 2018)).

IV. Conclusion

We hold that geofence warrants are modern-day general warrants and are unconstitutional under the Fourth Amendment. However, considering law enforcement's reasonable conduct in this case in light of the novelty of this type of warrant, we uphold the district court's determination that suppression was unwarranted under the good-faith exception.

AFFIRMED.

Here, Moody testified about two technological areas: (1) CSLI; and (2) Google Location History. First, Appellants acknowledge that this court has accepted historical cellular site analysis in the past as the subject of expert testimony. *See United States v. Schaffer*, 439 F. App'x 344, 347 (5th Cir. 2011). Second, it is undisputed that Google Location History is a collection of data that is itself derived from a combination of three forms of geolocation—CSLI, GPS, and Wi-Fi. Thus, Moody's extensive knowledge, skill, experience, training, and education in historically reliable forms of geolocation, such as CSLI, GPS, and Wi-Fi, allowed him to discuss Google Location History data, which is itself derived from those very sources. At bottom, the district court did not commit error, let alone manifest error, by allowing Moody to testify.

JAMES C. HO, *Circuit Judge*, concurring:

Geofence warrants are powerful tools for investigating and deterring crime. The defendants here engaged in a violent robbery—and likely would have gotten away with it, but for this new technology. So I fully recognize that our panel decision today will inevitably hamper legitimate law enforcement interests.

But hamstringing the government is the whole point of our Constitution. Our Founders recognized that the government will not always be comprised of publicly-spirited officers—and that even good faith actors can be overcome by the zealous pursuit of legitimate public interests. "If men were angels, no government would be necessary." THE FEDERALIST No. 51, at 349 (J. Cooke ed. 1961). "If angels were to govern men, neither external nor internal controls on government would be necessary." *Id.* But "experience has taught mankind the necessity of auxiliary precautions." *Id.* It's because of "human nature" that it's "necessary to control the abuses of government." *Id.*

Our decision today is not costless. But our rights are priceless. Reasonable minds can differ, of course, over the proper balance to strike between public interests and individual rights. Time and again, modern technology has proven to be a blessing as well as a curse. Our panel decision today endeavors to apply our Founding charter to the realities of modern technology, consistent with governing precedent. I concur in that decision.

United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
January 14, 2025
Lyle W. Cayce
Clerk

No. 23-60321

UNITED STATES OF AMERICA,

Plaintiff—Appellee,

versus

JAMARR SMITH; THOMAS IROKO AYODELE; GILBERT MCTHUNEL, II,

Defendants—Appellants.

Appeal from the United States District Court
for the Northern District of Mississippi
USDC No. 3:21-CR-107-1

ON PETITION FOR REHEARING EN BANC

Before KING, HO, and ENGELHARDT, *Circuit Judges*.

PER CURIAM:

Treating the petition for rehearing en banc as a petition for panel rehearing (5TH CIR. R. 35 I.O.P.), the petition for panel rehearing is DENIED. Because no member of the panel or judge in regular active service requested that the court be polled on rehearing en banc (FED. R. APP. P. 35 and 5TH CIR. R. 35), the petition for rehearing en banc is DENIED.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
OXFORD DIVISION

UNITED STATES OF AMERICA

v. CRIMINAL CASE NO. 3:21-cr-107-SA

JAMARR SMITH, THOMAS AYODELE,
and GILBERT MCTHUNEL DEFENDANTS

ORDER AND MEMORANDUM OPINION

On November 4, 2022, Jamarr Smith filed a Motion to Suppress [74]. Thomas Ayodele and Gilbert McThunel filed Joinders to the Motion [74]. *See* [76, 79]. The Defendants seek to suppress all evidence derived from the November 2018 geofence warrant which was used to identify them as suspects of a robbery that took place in February 2018. The Court held a hearing on the Motion [74] on January 31, 2023. Having considered the evidence presented at the suppression hearing, as well as the parties' filings and applicable authorities, the Court is prepared to rule.

Factual Background

The parties agree as to many of the underlying facts that led to the Indictment [1] being filed against the Defendants.

Around 5:25 PM on February 5, 2018, a U.S. Postal Service Highway Contract Route Driver, Sylvester Cobbs, was robbed as he was picking up mail from the Lake Cormorant Post Office, in Lake Cormorant, Mississippi. Cobbs' job as a driver consisted of picking up mail from the Dundee, Tunica, Robinsonville, Lake Cormorant, and Walls, Mississippi Post Offices and transporting mail to the Processing and Distribution Center in Memphis, Tennessee.

According to Cobbs, on the day in question, he was parked in the parking lot of the post office when he was approached from behind by an unknown African American male wearing a black long-sleeve shirt and a black ski mask who was approximately 5'9" to 6'0" tall. The man pointed a handgun at Cobbs with one hand and some form of mace with the other. The man then attempted to lock Cobbs inside the vestibule of the post office; however, Cobbs fought back with the man and the man pistol whipped Cobbs several times in return. After that, according to Cobbs, the man went to the back of the mail truck and took three registered mail sacks, which contained $60,706. The man also took Cobbs' post office keys. Thereafter, the man fled, and Cobbs drove his truck across the street to call his wife and postal management.

No suspect was arrested in connection to the robbery on the day of occurrence. However, in the following days, Postal Inspectors retrieved surveillance footage from a camera located at a nearby farm office. The camera captured the robbery on video. The video showed a red Hyundai (believed to be an Elantra) and a large white SUV (believed to be a newer model GMC Yukon XL) in the area. The video revealed the suspect getting out of the SUV before the robbery, and it is inferred that the suspect got back into the SUV before fleeing the scene. According to Todd Matney's (inspector of the United States Postal Inspection Service) affidavit in support of his search warrant application, the "Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs." [74], Ex. 2 at p. 4. Stephen Mathews (former Postal Inspector and supervisor of the Oxford, Mississippi Postal Inspector's Office) testified at the hearing that he interviewed Cobbs, who was unable to identify any suspects because the suspect was wearing a

ski mask.[1] Sometime after obtaining the video footage, but prior to applying for the warrant, Mathews located an eyewitness who lived across the street. According to Mathews, the witness asked the driver of the red Hyundai if he needed any help. The driver informed the eyewitness that he was looking for Highway 61. At this point in time, the witness was unable to identify the driver of the car.[2]

On November 8, 2018 (nine months after the robbery), Inspector Matney applied for a search warrant seeking information from Google to locate potential suspects and witnesses in connection to the February robbery. This specific type of warrant is known as a geofence warrant. According to Inspector Matney, he worked with Mathews, spoke with other investigators from other states who had applied for geofence warrants, and consulted with the United States Attorney's Office in Oxford, Mississippi before applying for the geofence warrant.

A geofence warrant is a fairly new investigative technique, wherein law enforcement request's location data from a third-party, such as Google. This type of warrant allows law enforcement to rely on technology to locate unknown potential suspects and witnesses of a crime. Attached to the Defendants' Motion to Suppress [74] is Spencer McInvaille's (the Defendants' expert) report which sets forth a three-step process that Google follows when responding to a geofence warrant. [74], Ex. 4.[3]

[1] For context, Mathews was the supervisor of the Postal Inspector's Office in Oxford, Mississippi in 2018—the time the warrant was applied for. At the time of the hearing, and currently, Mathews is no longer an active law enforcement officer. Therefore, the Court will hereinafter not refer to Mathews as an "Inspector."
[2] Mathews testified that after the three suspects were arrested (several months later), he presented the eyewitness with three separate photo lineups to see if the eyewitness could identify any of the suspects. Although the eyewitness was unable to identify McThunel or Smith in their respective lines, the eyewitness did identify Smith as the person he saw driving the red Hyundai.
[3] While the parties, to some extent, dispute the information returned from the geofence warrant in this case, the parties do not dispute the three-step process Google follows when it responds to a geofence warrant.

According to the report, a geofence warrant demands that Google search its database, known as the Sensorvault, to locate unknown suspects of crime. At the outset, law enforcement provides Google with geographical and temporal parameters around the time and place where the alleged crime occurred. The first step requires Google to search its Sensorvault for *all* users who have location history enabled at the time the warrant was executed. At the hearing McInvaille testified that, when acting in accordance with a geofence warrant, Google searches data for all users who had their location history enabled because the data itself is not capable of being stored in a way to search a specific area. Thus, Google searches all location history stored in its Sensorvault. Google describes the location history as a "[p]ersonal and private journal of the user's location." *Id.* at p. 1. To be clear, location history is not automatically enabled. A user must opt-in to sharing his or her location history either through phone set up or through an app.

After Google searches the Sensorvault and determines the accounts that were within the geographical parameters of the warrant, it returns to law enforcement a list giving each account an anonymized device ID, also including the date and time, longitude and latitude, the source, and the maps display radius. According to the report, "the maps display radius is indicated in meters and the radius is drawn around the center point referenced with the latitude and longitude" and "Google estimates the device should be located within the circle and states that their goal is for that to be true 68% of the time." *Id.* at 5. During the hearing, the Government introduced an exhibit illustrating this process, and McInvaille provided testimony explaining it in more detail.

Step Two is a request for contextual data. During this step, law enforcement reviews the anonymized list and determines which device IDs are relevant to the investigation. Then, law enforcement can request additional de-anonymized information that goes beyond the parameters of the initial geofence. According to Google, the purpose of this step is to potentially eliminate

false positives or determine if a device ID is relevant. *Id.* at p. 7. This step also allows law enforcement to compel Google (if authorized in the request) to provide account-identifying information, such as an email address, for the device IDs that law enforcement deems relevant.

In the third step, Google produces the subscriber's information for the accounts that were determined relevant in Step Two. This data is provided in a de-anonymized format which includes email addresses from Step Two, along with the names associated with the device IDs.

After the magistrate judge approved the warrant, Inspector Matney submitted the warrant to Google. Inspector Matney testified that, submitting the warrant to Google required him to access a legal portal and sign in with a government email address. After he signed in, Inspector Matney was able to upload the warrant and any subsequent documents through the portal.

Attached to the warrant was "Attachment A." Section II of the attachment outlined the three-step process that Inspector Matney submitted to the magistrate judge for his approval. Section II specifically provided:

> To the extent within the Provider's possession, custody, or control, the provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.
>
> 1. Location Information. All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018;
> 2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical

> identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.
> 3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine the path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of the path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)
> 4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

[74], Ex 3 at p. 2.[4]

As this quoted language illustrates, the language of the warrant largely tracks Google's three-step process outlined above. After receiving the warrant, Google followed its three-step process. Although the precise number of user accounts searched is unclear, Google estimated that number to be around 592 million accounts at the time the warrant was executed. The warrant authorized an hour-long search from 5:00 PM to 6:00 PM on February 5, 2018. The geofence covered approximately 98,192 square meters around the Lake Cormorant Post Office. The warrant, consistent with Step Two, authorized law enforcement to obtain additional location history for a registered device "60 minutes plus or minus the first and last timestamp associated with the account

[4] Although this Section II information was not attached to the copy of the warrant attached to the Motion to Suppress [74], this appears to have been an oversight when the Motion [74] was initially filed. This issue was addressed at the hearing, and the Court has reviewed the official copy of the original warrant and notes that Section II *was* in fact part of the warrant.

in the initial dataset." *Id.* Google returned Step One information in April 2019. This step returned three device IDs (in an anonymized format) within the requested parameters (with two of the three devices registering multiple times). *See diagram below*. Inspector Matney testified that he then reviewed the device IDs to ensure they fell within the geofence coordinates.

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radium (m)
1091610859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091610859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091610859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091610859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091610859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

At this point, the parties' versions of events diverge. The Defendants contend that, before receiving Step Two data, law enforcement did not follow the applicable Step Two narrowing measures. Instead, without obtaining an additional warrant (which the Defendants contend violated the "further legal process" language in the warrant), Inspector Matney and Mathews decided which device IDs were relevant and requested additional de-anonymized information for all three devices. Although, the Defendants, along with McInvaille, contend that it appeared Step Two had been skipped and it was not contained in discovery, Inspector Matney testified at the hearing that, in May 2019, he requested Step Two data through the portal. According to Inspector Matney, he, along with Mathews, decided that the device IDs ending in "859" and "768" were relevant because those devices registered multiple times within the geofence. They decided the third device ID, which only registered one time within the geofence, could have been a potential witness, but ultimately was not relevant to the investigation. Inspector Matney testified that on May 30, 2019,

Google sent law enforcement a letter containing Step Two data. There was also testimony that the Step Two narrowing measures took place with a subsequent warrant (discussed below) obtained in July 2019. During this step, according to the Government, Google also expanded the search to include the additional location history on the registered devices, as authorized in the warrant.

At the beginning of June 2019, Inspector Matney was injured, requiring a leave of absence from work, and Mathews took over as the lead investigator. Mathews testified that he received Step Three data around June 10, 2019. This data included de-anonymized information for *all* three devices IDs. The following email address were returned:

"2165781.Key.cvs",

"bleek2004.AccountInfo.txt",

"jamarrsmith33.AccountInfo.txt", and

"permanentwavesrecords.AccountInfo.txt."[5]

Through the information he received from Google, Mathews determined that the "jamarrsmith33.AccountInfo.txt" was Smith's email account and the "bleek2004.AccountInfo.txt" email account belonged to McThunel. At the hearing, Mathews testified that the email "permanentwavesrecords.AccountInfo.txt", which was associated with the third device, was deemed irrelevant to the investigation.

According to Mathews, he submitted another warrant (Google warrant) in the middle of July 2019. To be clear, this was *not* a geofence warrant, but instead sought location information as to those specific Google accounts that he had previously determined belonged to Smith and McThunel. Mathews testified that this warrant authorized specific location information connected

[5] Although this appears to be four separate email addresses, at the hearing, no reference was made to the "2165781.Keys.cvs" account. It is unclear to the Court what that email might reference. Nevertheless, it was clear at the hearing that the parties agree law enforcement only received de-anonymized information associated with three accounts—not four.

to Smith and McThunel's accounts and showed them traveling from Batesville, Mississippi to Lake Cormorant, Mississippi on the day of the robbery. Mathews also obtained phone records on all three suspects. The phone records revealed a 350 second phone call between Smith and McThunel during the time of the robbery. The phone records also indicated a phone call between Ayodele and McThunel, which is how Ayodele was identified as a third suspect.

Ultimately, the Government was able to identify the three Defendants and obtain an Indictment [1] against them. In the Motion to Suppress [74], the Defendants argue that the geofence warrant was invalid from its inception because it lacked probable cause and particularity. The Defendants also take the position that they had a reasonable expectation of privacy in their location history and that the geofence warrant violated that reasonable expectation. Furthermore, the Defendants argue that, in the event that the warrant was valid, the Government did not undertake "further legal process" to obtain additional information from Google as it said it would do, which made Steps Two and Steps Three of the search warrantless and illegal. Finally, they argue that the good faith exception set forth in *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984) does not excuse the defects of the warrant. They contend that the exclusionary rule should apply and that all the evidence seized constitutes "fruit of the poisonous tree."

Applicable Standard

"The defendant challenging a search must show the warrant to be invalid by the preponderance of the evidence." *United States v. Richardson*, 943 F.2d 547, 548 (5th Cir. 1991) (citing *United States v. Osborne*, 630 F.2d 374, 377 (5th Cir. 1980)). "That burden includes establishing standing to contest the evidence, and showing that the challenged government conduct constitutes a Fourth Amendment search or seizure." *United States v. Turner*, 839 F.3d 429, 432

(5th Cir. 2016). However, "when the government searches or seizes a defendant without a warrant, the government bears the burden of proving by a preponderance of the evidence, that the search or seizure was constitutional." *United States v. Guerrero-Barajas*, 240 F.3d 428, 432 (5th Cir. 2001).

Analysis and Discussion

The Fourth Amendment assures the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Moreover, "no warrants shall issue, but upon probable cause, supported by oath and affirmation, and particularly describing the place to be searched, and the persons or thing to be seized." *Id.* The Fourth Amendment requires that a search warrant be issued only when there is probable cause to believe that an offense has been committed and that evidence exists at the place for which the warrant is requested. *United States v. Place*, 462 U.S. 696, 701, 103 S. Ct. 2637, 2641, 77 L.Ed.2d 110 (1983). If a warrant is invalid, the appropriate remedy is to suppress the evidence obtained through an unreasonable search or seizure. *United States v. Beaudion*, 979 F.3d 1092, 1097 (5th Cir. 2020).

As noted above, the Defendants raise several arguments as to the purported unconstitutionality of the geofence warrant and, consequently, the inadmissibility of the evidence obtained therefrom. Specifically, the Defendants contend they had a reasonable expectation of privacy in their data obtained through the warrant, the warrant lacked probable cause and particularity, and that the good faith exception is inapplicable. The Court will address the issues in turn.[6]

[6] The Court notes that, in its Response [87], the Government raised an argument that the Defendants' lacked standing. The Government did not raise this issue at the hearing and, perhaps, concedes this point. Nevertheless, the Court does not find the argument persuasive, as it is undisputed that the location history of both Smith and McThunel was obtained through the execution of the geofence warrant. Therefore, they have standing.

A. Reasonable Expectation of Privacy

Beginning first with the issue of reasonable expectation of privacy, the Defendants contend that they possessed a reasonable expectation of privacy in their location history. The Defendants rely on *Carpenter v. United States*, wherein the Supreme Court specifically rejected the application of the third-party doctrine on the basis that, given the unique nature of cellphone data, users do not truly voluntarily share their data with a third party. 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). On the other hand, the Government takes the position that because a user voluntarily opts-in to sharing his location history they maintain no reasonable expectation of privacy. The Government further contends that obtaining two hours of the Defendants' location history is not the same as the seven days' worth of information obtained in *Carpenter* (which the Supreme Court later determined violated the defendant's reasonable expectation of privacy).

Other district courts have grappled with the privacy concerns that geofence warrants raise. The District Court for the Eastern District of Virginia, analyzing the constitutionality of a geofence warrant, declined to delve too deeply into the issue of whether the defendant possessed a reasonable expectation of privacy in his location history data obtained through the geofence warrant because the court found that the good faith exception applied. *United States v. Chatrie*, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022). Although the *Chatrie* court did not reach a determination on the reasonable expectation of privacy issue, the court acknowledged its deep concerns with geofence warrants and stated that the "[c]urrent Fourth Amendment doctrine may be materially lagging behind technological innovations." *Id.* Most recently, the District Court for the District of Columbia followed the *Chatrie* court's reasonable expectation of privacy analysis. *United States v. Rhine*, 2023 WL 372044, at *28 (D.D.C. Jan. 24, 2023). Recognizing the novelty

of warrants of this nature and for reasons set forth more fully hereinafter, the Court need not definitively resolve that issue.

B. Probable Cause

Next, the Defendants contend that the geofence warrant is wholly invalid because it lacked sufficient probable cause. The Supreme Court has held that probable cause requires a "[f]air probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332, 76 L. Ed. 2d 527 (1983). Furthermore, a warrant must not be overbroad. *United States v. Sanjar*, 853 F.3d 190, 200 (5th Cir. 2017) (citing *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009)). This requires probable cause to seize the particular things named in the warrant. *Id.* More specifically, the Fourth Amendment requires "that (1) a warrant provide sufficient notice of what the agents may seize and (2) probable cause exists to justify listing those items as potential evidence subject to seizure." *Sanjar*, 853 F.3d at 200 (citing *William v. Kunze*, 806 F.2d 594, 598-99 (5th Cir. 1986)).

The Defendants contend that the geofence warrant was not supported by probable cause because the warrant was overbroad. Specifically, the Defendants argue that the warrant did not identify any suspects and that the Government only learned the identity of the suspects via inverted probable cause. In their Memorandum [75], as well as at the hearing, the Defendants maintained that their probable cause argument was synonymous to *Ybarra v. Illinois*, 444 U.S. 85, 100 S. Ct. 338, 62 L. Ed. 2d 238 (1979), wherein the Supreme Court struck down a search warrant because although "the police did have probable cause to search the tavern where [Ybarra] happened to be when the warrant was executed, [] a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." 444 U.S. 85, 86, 100 S. Ct. 338, 339, 62 L. Ed. 2d 238 (1979). Although *Ybarra* addresses the physical

search of a person, the Defendants contend that the search of the tavern in *Ybarra* is synonymous to a search of Google's Sensorvault.

Conversely, the Government contends that Inspector Matney's affidavit in support of the warrant application contained more than enough information to establish probable cause. Particularly, the affidavit established that unknown suspects aided and abetted each other in committing the robbery. The affidavit also established a connection between Google location information and smartphones. Additionally, though the Government does not believe it was necessary, the affidavit stated that an unknown person was *possibly* using a cellphone before and after the robbery. Therefore, the Government contends that the affidavit included enough information to establish probable cause.

To aid its probable cause analysis, the Court considers the reasoning from *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) ("*Google III*"). There, the Government applied for a geofence warrant to investigate a series of arsons. *Id.* at 351. The geofence covered only a 15–30 minute time frame and only included the location of the arson sites, while excluding any irrelevant residential or commercial buildings. *Id.* at 357-58. The court concluded that the Government satisfied any overbreadth concerns by ensuring probable cause for location data on the suspects through "[o]n-site investigation, open source searches, and surveillance footage." *Id.* at 359. The magistrate judge determined that the warrant established sufficient probable cause and was not overbroad because the geofence only focused on the arson sites and structured geographical and temporal limitations in a manner to minimize capturing location data for uninvolved individuals. *Id.* at 357. The *Google III* court also noted that it was not necessary that

the affidavit contain information that the suspect possessed a phone during the commission of the crime to retrieve cellphone data. *Id.* at 355.

To further support its argument, the Government relies on *In re Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62 (D.D.C. 2021) ("*Google V*"). In *Google V*, the Government applied for a geofence warrant around a building where the Government alleged federal crimes had occurred. *Id.* at 72. The geofence only covered a portion of the front half of the building and did not include any other structures. *Id.* The geofence was approximately 875 square meters. *Id*. The district court concluded that the warrant established sufficient probable cause because "[t]here [was] a fair probability that the search of Google's servers [would] uncover useful evidence—i.e., the identities of the suspects inside the [building]". *Id.* at 77. Further, there was evidence that the suspects were using their cellphones while inside the building. *Id.* at 78. The court ultimately concluded that because the geofence was tailored to the building the location information that Google would return would not include an unnecessarily broad number of uninvolved individuals. *Id.* at 80.

Against this backdrop, the Court turns to the facts of this case. Although the parameters of the geofence were relatively large in scope, the geofence was in a rural area where it was unlikely to return a large number of Google accounts. Moreover, the affidavit contained additional evidence that the suspect was possibly using a phone, and this Court agrees with Inspector Matney's characterization that the suspect was *possibly* using a phone. Although the Court makes no definitive determination as to whether the evidence of cellphone use is necessary, the Court finds, based on the facts of this case, that the statement aided the Government in establishing probable cause. The affidavit also established a connection between smartphones and Google. The

Government established sufficient probable cause that indicated Google possessed data that would reveal suspects of the robbery.

In essence, the Defendants' argument on this point seems to be a contention that geofence warrants in general violate the Fourth Amendment. The Court declines to make such a sweeping determination.

The Court finds that the geofence warrant contained sufficient probable cause. To the extent the Defendants' Motion [74] seeks suppression on that basis, it is DENIED.

C. Particularity

A search warrant must describe the items to be seized "[w]ith sufficient particularity such that the executing officer is left with no discretion to decide what may be seized." *Kunze*, 806 F.2d at 598 (citing *Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed 231 (1927)).

The Defendants argue that the geofence warrant lacked particularity because it was not particular in the places to be searched or things to be seized. In their Motion [74], as well as at the hearing, the Defendants raise two arguments as to the particularity requirement. First, the Defendants argue that the geofence warrant failed to identify any particular suspects and that the magistrate judge would have never signed off on the warrant had he known it included a search of 592 million Google accounts. Second, the Defendants contend that the Government obtained additional information and decided which accounts to search in Steps Two and Three of Google's process and did so without obtaining an additional warrant, as required by the "further legal process" language in the warrant. Conversely, the Government contends that the warrant was tailored to the investigation and "[w]as narrowly constrained based on location, date, and time." [87] at p. 15. Moreover, as articulated by the Government, the warrant only sought location history for a total of two hours and was only searching for "[i]ndividuals present at the site of the robbery." [87] at p. 15. The Government further contends that the initial geofence warrant did not require

the agents to go back to the Court to obtain an additional warrant for Steps Two and Three. Instead, according to the Government, the phrase "upon demand", which is included in the warrant, meant upon the request from law enforcement and constituted the "further legal process" required under the warrant.

To support their particularity argument, the Government relies on the rationale from *United States v. James*, 2019 WL 325231 (D. Minn. Jan. 25, 2019.) In *James*, the Court authorized law enforcements use of cellphone "tower dumps" to locate suspects of a robbery. *Id*. at *1. The Court ultimately upheld the use of tower dumps because, through geographical and temporal parameters, the warrant was particular to the information sought. When asked about the difference between cellphone tower dumps and Google location history during the hearing, McInvaille explained that tower dumps provide data restricted to the location of the towers, whereas location history is stored in a way that requires Google to search *all* location history and not just a specific area. In other words, for a tower dump, the search can be limited to users in close proximity to a particular tower, whereas that same limitation cannot be accomplished in connection with a geofence warrant.

The Court again relies on *Google III* and *Google V*. In *Google III*, the magistrate judge found that the warrant met the particularity requirements because it narrowly identified the place to be searched by time and location limitations. *Google III*, 479 F. Supp 3d at 357. As noted above, the geofence only included a 15-30 minute timeframe and excluded residences and commercial buildings. *Id.* The *Google V* court reached the same conclusion for similar reasons. *Google V*, 579 F. Supp. 3d at *80. The district court found that the geofence contained sufficient temporal and geographic windows for the location data that was being sought. *Id.*

The Court notes the *Rhine* court (the most recent decision deciding the constitutionality of geofence warrants) also concluded that the geofence warrant at issue in that case met the particularity requirements. *Rhine*, 2023 WL 372044 at *32.

Here, the initial time period authorized by the warrant was limited to one hour and only authorized the retention of additional location history for a 60 minute time period for registered devices. The geofence encompassed the area in which the crime occurred. Furthermore, the affidavit specifically includes the latitude and longitude coordinates of where the crime occurred and states that "this application seeks authority to collect certain location information related to Google Accounts that were located within the Target Area during the Target Time Period." [74], Ex. 2 at p. 6. Simply put, this geofence contained similar temporal restrictions to the geofence warrants in *Google III* and *Google V*. The Court notes the stark difference in the geographical ranges of the geofence in *Google V* and the one presently before the Court. Here, the geofence is 98,192 square meters—a drastically larger difference than the 875 square meter geofence in *Google V*. However, considering that the geofence in the case at bar was in a rural area where there was an unlikely chance that a substantial number of uninvolved people would be captured in the geofence, the geographical size of the geofence does not cause this Court great concern.

In making that determination, the Court again finds it necessary to provide a qualification. The Court's determination on that point should not be interpreted as a determination that a geofence of 98,192 square meters is always permissible. In fact, there may very well be circumstances where it is not. The Court's determination is limited to the facts at issue here. A case-by-case analysis is appropriate.

Therefore, for reasons set forth above, the Court does not find the Government's tower dump argument directly on point, but does agree with the Government's overall position that the warrant was particular in identifying the places to be searched and things to be seized.

Next, the Defendants argue that, by not obtaining an additional warrant before obtaining additional information in Steps Two and Three, law enforcement did not comply with the "further legal process" language contained in the warrant. Therefore, the Defendants assert that the information obtained from Steps Two and Three is not particular. The court in *Google II* emphasized that "a warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize." *Google II*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020). There, the warrant did *not* require law enforcement to obtain an additional warrant for Steps Two and Three. *Id.* Therefore, the *Google II* court rejected the Government's particularity argument on the basis that the warrant was not narrowly tailored in a manner justified by the investigation. *Id.* In *Google V*, the magistrate judge reasoned that the warrant was valid because it required law enforcement to obtain further authorization from the court before receiving de-anonymized information on the Google accounts at Step Two. *Google V*, 579 F. Supp. 3d at 87. The *Google V* court further held, that any overbreadth concerns would be cured in the additional warrant obtained prior to receiving Step Two data. *Id.* Other Courts have criticized the lack of a requirement for additional authorization as providing law enforcement unbridled discretion. *See Google I*, 2020 WL 5491963 at 6; *Google II*, 481 F. Supp. 3d at 746; *Chatrie*, 590 F. Supp. 3d at 927.

Here, the Court finds that law enforcement did not follow the narrowing measures set forth in Step Two of Google's process. In fact, testimony from the hearing indicated that law enforcement did not narrow their investigation until the subsequent July 2019 warrant was obtained. This was a clear failure to follow the narrowing measure outlined in Step Two. Moreover,

without further authorization from the Court, Inspector Matney and Mathews chose which device IDs were of interest. During the hearing, McInvaille testified that Step Two of Google's approach was a narrowing measure that, without further authorization from a judge, gave law enforcement the discretion to choose which accounts were relevant. According to the Defendants, this cuts against the plain language contained in the warrant where it states that law enforcement "[w]ill seek any additional information regarding those devices through further legal process." [74], Ex. 3 at p. 2. On the other hand, the Government argued that further legal process was "upon demand" from law enforcement, not an additional warrant from the Court. In other words, the Government takes the position that "further legal process" was outlined in the later parts of Section II of Attachment A to the Warrant. Inspector Matney and Mathews additionally testified that they interpreted the "further legal process" language to mean that Google would produce additional information "upon demand" from law enforcement because the magistrate judge had already signed off on the initial warrant that included all three steps. To support that belief, Mathews testified that he resubmitted "Attachment A" (which was submitted along with the original warrant) instructing Google to comply with paragraph three of the attachment which states, "[a]nd upon demand, the 'Provider' shall provide additional location history. . ." [74], Ex 3. at p. 2.

As an initial matter, the Court disagrees with the Government's interpretation of the "further legal process" language. Furthermore, it was admitted at the hearing that the Government did in fact receive de-anonymized information for *all three* device IDs—even though, in its Response [87], as well as at the hearing, the Government maintained the position that only two of the device IDs were relevant to their investigation.

Although the Court rejects the Government's interpretation of the "further legal process" language, the Court does not question the credibility of Inspector Matney's nor Mathews'

testimony on that issue. In other words, the Court concludes that Inspector Matney and Mathews made a good faith interpretation that the "further legal process" language did not require them to return to the Court for an additional warrant before receiving Steps Two and Three data.

At the hearing, McInvaille testified that the "further legal process" language has shown up in other warrants and when it has, courts have interpreted that to mean that law enforcement must return to the court for authorization between each step of the Google process. He provided specific examples of other cases.

Ultimately, the Court makes no determination as to whether geofence warrants are per se constitutional but, instead, finds that a case-by-case determination is appropriate in determining the appropriate geographic parameters. In reaching its conclusion, the Court notes, and the parties agreed at the hearing, that in November 2018, the time law enforcement applied for the geofence warrant, there was no published case law on the constitutionality of geofence warrants. The Court finds that fact—and the novelty of geofence warrants as a whole, particularly at the time of Inspector Matney and Mathews' relevant conduct—to be important in analyzing this case.

The Court rejects the Defendants' argument that the warrant was so overbroad as to render it unconstitutional. But the Court does find that "further legal process" required law enforcement to obtain an additional warrant before requesting Steps Two and Steps Three data. The Government admits that no such warrant was obtained. Consequently, the critical determination becomes whether that failure warrants suppression or, as the Government contends, the good faith exception should apply.

D. Good Faith Exception

"The good faith exception to the exclusionary rule provides that 'evidence obtained during the execution of a warrant later determined to be deficient is nonetheless admissible if the executing officer's reliance on the warrant was objectively reasonable and made in good faith.'"

United States. v. Massi, 761 F.3d 512, 525 (5th Cir. 2014) (citing *United States v. Woerner*, 709 F.3d 527, 533 (5th Cir. 2013)) (additional citation omitted). "Applying the good-faith exception does not resolve whether a constitutional right has been violated; it simply is a judicial determination that exclusion of evidence does not advance the interest of deterring unlawful police conduct." *Id*. (citing *Leon*, 468 U.S. at 906-07, 104 S. Ct. 3405; *Gates*, 462 U.S. at 223, 103 S. Ct. 2317). "In effect, the good-faith exception limits the remedy of exclusion where the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." *Id.* (citing *Leon*, 468 U.S. at 922, 104 S.Ct. 3405).

In *Leon*, the Supreme Court articulated four circumstances where the good faith exception does not apply: "1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; 2) when the issuing magistrate wholly abandoned his judicial role; 3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and 4) when the warrant is so facially deficient in failing to particularize the place to be searched or things to be seized that executing officers cannot reasonably presume it to be valid." 468 U.S. at 899, 104 S. Ct. 3405. The good faith exception analysis is focused on "[w]hether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003) (citing *Leon*, 468 U.S. at 922 n. 23, 104 S. Ct. 3405).

The Defendants contend that the good faith exception is not implicated here because three of the four circumstances articulated above are applicable. The Government disagrees and contends that the good faith exception should apply. Particularly, the Government relies on two

separate arguments on this point—first, under the holding from *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018); and second, from the traditional good faith exception articulated in *Leon*.

First, the Defendants contend that the good faith exception does not apply because the affidavit contained a misrepresentation that Inspector Matney knew or should have known was false. The Defendants base this argument on the rationale set forth in *Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667. To prove this claim under *Franks*, the Defendants must show that (1) the affidavit supporting a warrant contained false statements or material omissions; (2) the affiant made such false statements or omissions knowingly and intentionally or with reckless disregard for the truth; and (3) the false statements or material omissions were necessary to the finding of probable cause. *Davis v. Hodgkiss*, 11 F.4th 329, 333 (5th Cir. 2021) (citing *Franks*, 438 U.S. at 155-56, 98 S. Ct. 2674) (additional citations omitted).

The portion of the affidavit in question, which ultimately, at least in part, led to the issuance of the geofence warrant, states that "Postal Inspectors conducted a detailed review of the video surveillance and *it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs.*" [74], Ex. 2 at p. 4. (emphasis added). The Defendants contend they meet the first two prongs of the *Franks* analysis because the video footage does not show a cellphone, making Inspector Matney's statement intentionally reckless. According to the Defendants, a more accurate statement would have read that "[i]t *does not* show the robbery suspect using a cellular device before or after the robbery occurs." [75] at p. 12. (emphasis added). Because of this, the Defendants argue that the statement is reckless.

At the hearing, Inspector Matney testified that there were several times during the video where the assailant's body language appeared to be consistent with talking on the phone. First, around the 6:50 minute mark. During this time, the assailant's arm appeared to be raised up to his

left ear for several minutes. Next, around the 13:34 minute mark, the assailant is seen crouching on the ground and making a movement that Inspector Matney believed was consistent with sending or checking a text message.

After reviewing the video footage and testimony from the hearing, the Court rejects the Defendants' argument that Inspector Matney stating the assailant is possibly using a cellphone is outright false. Although there is never a cellphone shown on the video, the Court finds the statement was not a misrepresentation and that Inspector Matney's interpretation of the video could have led him to believe that the assailant's body language was consistent with using a cellphone. The Defendants' contentions as to the language they would have preferred Inspector Matney to have used are unavailing. The Court does not find that Inspector Matney made a knowing misrepresentation.

Next, the Defendants argue that the good faith exception is not applicable because the warrant lacked probable cause and the warrant was facially deficient because it did not meet the particularity requirements. In its analysis above, the Court has already concluded that there was sufficient probable cause and that the particularity requirement was met. The Court sees no need to recite that analysis again and will not address those issues any further.

Ultimately, the Court finds the Fourth Circuit's reasoning in *McLamb* persuasive. In *McLamb*, the Fourth Circuit declined to find a warrant facially deficient when law enforcement faced with novel investigative techniques consulted with counsel prior to applying for a warrant. *McLamb*, 880 F.3d at 691. Here, included in the affidavit, Inspector Matney stated that he had conversations with other law enforcement officers before submitting the geofence warrant. In its Response [87], the Government also states that Inspector Matney consulted with the United States Attorney's Office prior to submitting the warrant. Inspector Matney's testimony on this point was

consistent with the Government's contention. Furthermore, throughout the hearing, it became abundantly clear that neither Inspector Matney nor Mathews had personal experience with geofence warrants when they applied for the present warrant. They both explained multiple steps that they took to attempt to undertake the inspection properly—such as consulting with an Assistant United States Attorney, communicating with other agencies across the country, and reviewing similar warrant templates. The Court found their testimony to be credible insofar as it concerned the steps they believed they were required to take in connection with the geofence warrant. Inspector Matney's testimony on this point was consistent with the Government's contention.

The Court also finds noteworthy the rationale underlying the good faith exception. *See Herring v. United States*, 555 U.S. 135, 145, 129 S. Ct. 703, 172 L.Ed.2d 496 (2009) ("To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it. . ."). Here, the Court struggles to see any wrongful conduct to deter. Before seeking the warrant, Inspector Matney and Mathews consulted with the United States Attorney's Office and sought legal guidance, and the Court finds credible their testimony that they believe the warrant did not mandate that they return to the Court for an additional warrant. Ultimately, the conduct of law enforcement in this case seems reasonable and appropriate when considering the specific circumstances with which the investigators were faced.

Although the Court's ruling today will certainly create clear authority as to the meaning of "further legal process," Inspector Matney and Mathews, at the time they sought the warrant and acted in accordance with it, did not have any authority upon which to rely. In fact, counsel for both parties conceded that there was no published authority on this issue at the time. Even today, the

case law is sparse. Ultimately, the Court simply does not find that suppression in this case would further the rationale underlying the good faith exception.

Conclusion

For reasons set forth above, the Motion to Suppress [74] is DENIED.

SO ORDERED, this the 10th day of February 2023.

/s/ Sharion Aycock
UNITED STATES DISTRICT JUDGE

Supreme Court of the United States
Office of the Clerk
Washington, DC 20543-0001

Scott S. Harris
Clerk of the Court
(202) 479-3011

March 28, 2025

Mr. Goodloe Lewis
Hickman, Goza & Spragins, PLLC
1305 Madison Avenue
Oxford, MS 38655

Re: Jamarr Smith, Thomas Iroko Ayodele, and Gilbert McThunel, II
v. United States
Application No. 24A933

Dear Mr. Lewis:

The application for an extension of time within which to file a petition for a writ of certiorari in the above-entitled case has been presented to Justice Alito, who on March 28, 2025, extended the time to and including May 13, 2025.

This letter has been sent to those designated on the attached notification list.

Sincerely,

Scott S. Harris, Clerk

by

Pipa Fisher
Case Analyst

Supreme Court of the United States
Office of the Clerk
Washington, DC 20543-0001

Scott S. Harris
Clerk of the Court
(202) 479-3011

NOTIFICATION LIST

Mr. Goodloe Lewis
Hickman, Goza & Spragins, PLLC
1305 Madison Avenue
Oxford, MS 38655

Mrs. Sarah M. Harris
Acting Solicitor General
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Clerk
United States Court of Appeals for the Fifth Circuit
600 S. Maestri Place
New Orleans, LA 70130