

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

UNITED STATES OF AMERICA,

v.

TERRY BROWN (31),

Defendant.

CRIMINAL ACTION FILE NO.:

1:16-CR-427-AT-JKL-31

**ORDER AND FINAL REPORT AND RECOMMENDATION**

Defendant Terry Brown is charged with RICO (Racketeer Influenced and Corrupt Organizations Act) conspiracy, VICAR (Violent Crimes in Aid of Racketeering Activity) murder, and the death of a person through use of a firearm, related to his alleged involvement in the Nine Trey Gangsters (“NTG”) and the killing of Demetrius Davis. [Doc. 1158.] The case is presently before the Court on Mr. Brown’s motion to suppress evidence and perfected motion to suppress evidence obtained pursuant to three “geofence warrants.” [Docs. 1707, 1709.] Mr. Brown makes a Fourth Amendment challenge to the warrants, the first of which allowed law enforcement to collect Google location history (“LH”) information from a roughly 20-by-55-yard area during a 21-minute period. [See Doc. 1709-1, 1730-1.] The government has filed a response in opposition to the motions [Doc. 1730], and Mr. Brown has filed a reply [Doc. 1739]. For the reasons that follow,

it is **RECOMMENDED** that Defendant's motion to suppress evidence from search warrants 1:19-mc-1550, 1:20-mc-152, and 1:20-mc-364 be **DENIED**.<sup>1</sup>

## I. BACKGROUND

Geofence warrants are a relatively new and increasingly used tool that allow law enforcement to find out who was present at a crime scene by tapping into LH records from Google.<sup>2</sup> Law enforcement identifies a geographic location where criminal activity happened, draws a "geofence" around that area using coordinates

---

<sup>1</sup> Also pending before the Court is Defendant's Preliminary Motion to Suppress Evidence in which he moves to suppress evidence seized in connection with a search of a residence. [Doc. 1707.] The government has since filed a motion to withdraw its opposition to the motion to suppress, in which it represents that it will not use evidence gathered from the search of the residence in its case-in-chief. [Doc. 1754.] The motion to withdraw is **GRANTED**. Given the government's representation, it is unnecessary to evaluate the admissibility of that evidence and, thus, it is **RECOMMENDED** that the motion to suppress [Doc. 1707] be **DENIED AS MOOT**.

<sup>2</sup> See Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works*, N.Y. Times (Apr. 13, 2019), located at <https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html> (last visited Sept. 19, 2023); see also Google, *Supplemental Information on Geofence Warrants in the United States*, [https://services.google.com/fh/files/misc/supplemental\\_information\\_geofence\\_warrants\\_united\\_states.pdf](https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf) (last visited Sept. 19, 2023) (reporting that geofence warrants constitute more than 25% of all warrants received by Google in the United States); Brian L. Owsley, *The Best Offense Is A Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 Hofstra L. Rev. 829, 834 (2022) (explaining that the government applied for its first geofence warrant in 2016 and, in 2020, Google received over 11,500 geofence warrant requests for data).

on a map, and then seeks to identify the mobile phones (and their users) operating within that geofenced location within a particular span of time using Google’s LH information. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022). According to Google, users opt into the LH service, which functions as “essentially a history or journal” of a user’s “movements and travels” and is typically “captured in the ‘Timeline’ feature of the Google Maps app.” [Doc. 1709-6 at 10, 13 (Google Amicus Brief in *Chatrie*).]<sup>3</sup> Once a user opts into the service, his LH is logged, on average, every two minutes across every app and every device associated with the user’s account. *Chatrie*, 590 F. Supp. 3d at 908-09. Google LH information can show a device’s location “within approximately twenty meters.” [*Id.* at 17.]

The existing precedent concerning the validity of geofence warrants, and their collection of LH information, is “limited.” *United States v. Rhine*, \_\_ F. Supp. 3d \_\_, No.: 21-0687 (RC), 2023 WL 372044, at \*21 (D.D.C. Jan. 24, 2023). Six magistrate judges have addressed geofence warrants before issuance.<sup>4</sup> At least six

---

<sup>3</sup> This R&R uses CM/ECF numbering in its citations for all filings in this case.

<sup>4</sup> *See Matter of Search of Info. Stored at Premises Controlled By Google*, No. 2:22-MJ-01325, 2023 WL 2236493 (S.D. Tex. Feb. 14, 2023); *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 68 (D.D.C. 2021) (explaining why a geofence warrant was granted and, in

district court opinions have analyzed geofence warrants in the context of suppression motions.<sup>5</sup> But no federal appeals court, including the Eleventh Circuit, has yet ruled on this emerging area of the law, though two of the district court geofence cases are currently on appeal before the Fourth and Fifth Circuits. *See Smith*, 2023 WL 1930747, *appeal docketed*, No. 23-60321 (5th Cir. June 19, 2023); *Chatrie*, 590 F. Supp. 3d 901, *appeal docketed*, No. 22-4489 (4th Cir. Aug. 29, 2022). Accordingly, the undersigned begins with a review of relevant Fourth

---

turn, adding “to the limited federal caselaw discussing the legality of such warrants”); *Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1154 (D. Kan. 2021) (“The court issues this written order not only to address the subject application, but also to provide guidance for future search warrant applications involving geofence technology given the relatively sparse authority on this issue.”); *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A*, No. 20-M-297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

<sup>5</sup> *See United States v. Wright*, No. 4:19-CR-149, 2023 WL 5804161 (S.D. Ga. Sept. 7, 2023); *United States v. Scott Carpenter*, No. 8:21-CR-309-VMC-MRM, 2023 WL 3352249 (M.D. Fla. Feb. 28, 2023), *report and recommendation adopted*, 2023 WL 2910832 (M.D. Fla. Apr. 12, 2023); *United States v. Smith*, No. 3:21-CR-107-SA, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023), *appeal docketed*, No. 23-60321 (5th Cir. June 19, 2023); *Rhine*, 2023 WL 372044; *United States v. Davis*, No. 2:21-CR-101-MHT-JTA, 2022 WL 3009240 (M.D. Ala. July 1, 2022), *report and recommendation adopted*, 2022 WL 3007744 (M.D. Ala. July 28, 2022); *Chatrie*, 590 F. Supp. 3d at 901.

Amendment and geofence warrant cases to set the stage for an analysis of this case’s specific—and unique—geofence warrant.

#### **A. Relevant Precedent**

The Fourth Amendment protects 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. The government violates this amendment, then, when it invades anything to which a person has “a justifiable, a reasonable, or a legitimate expectation of privacy.” *United States v. Gayden*, 977 F.3d 1146, 1151 (11th Cir. 2020) (quotation marks omitted). In contrast, the Fourth Amendment is not infringed, or implicated, by a search of something in which an individual has no reasonable expectation of privacy. *United States v. Ross*, 964 F.3d 1034, 1040 (11th Cir. 2020). “This issue—whether an individual has a reasonable expectation of privacy in the object of the challenged search—has come to be known as Fourth Amendment ‘standing.’” *Id.*

Because Fourth Amendment standing is not a jurisdictional question, courts faced with geofence warrant challenges have largely skipped determining whether an individual has a reasonable expectation of privacy in LH information. *See Chattrie*, 590 F. Supp. 3d at 925 (declining to “wade into the murky waters of [Fourth Amendment] standing”). Instead, the analysis typically progresses as

follows: the Court conducts a review of the sufficiency of a challenged geofence warrant's probable cause and particularity and then usually denies the relevant suppression motion under the *Leon*<sup>6</sup> good faith exception to the exclusionary rule. *See, e.g., Scott Carpenter*, 2023 WL 3352249 at \*9<sup>7</sup>; *Smith*, 2023 WL 1930747 at \*8-12; *Rhine*, 2023 WL 372044 at \*27; *Chatrie*, 590 F. Supp. 3d at 929-30, 936-941. With the foregoing in mind, the Court reviews a number of relevant geofence warrant opinions in greater detail below.

### 1. *United States v. Chatrie*

In *Chatrie*, the first district court case analyzing geofence warrants after issuance, the challenged warrant had a geofence diameter of 300 meters in an urban environment, which included the scene of a bank robbery and a nearby church, and collected LH data for an hour-long period. 590 F. Supp. 3d at 918-19. It also sought information for another hour outside the geofence, without geographic restriction, from users who had been identified within the geofence. *Id.* at 929. In reviewing the warrant, the court determined that it lacked sufficient particularized

---

<sup>6</sup> *United States v. Leon*, 468 U.S. 897, 909 (1984) (creating the good faith exception to the exclusionary rule, in which evidence is admissible where law enforcement acted in good faith and suppression would not produce deterrent benefits).

<sup>7</sup> When citing to this case, the Court uses the defendant's first and last names to avoid confusion with the Supreme Court's decision *Carpenter v. United States*, 138 S. Ct. 2206 (2018), which the Court discusses below.

probable cause and “plainly violate[d] the rights enshrined” in the Fourth Amendment. *Id.* at 905, 929-30. Regardless, it denied a motion to suppress evidence obtained from that warrant under the *Leon* good faith exception. *Id.* at 936-41. The court also declined to answer whether the defendant had Fourth Amendment standing, but noted that the “expansive, detailed, and retrospective nature of Google location data . . . perhaps causes such data to cross the line from merely augmenting law enforcement’s investigative capabilities to impermissibly enhancing them.” *Id.* at 925-26 (cleaned up). The *Chatrie* court also expressed concerns that “current Fourth Amendment doctrine may be materially lagging behind technological innovations.” *Id.* at 925.

**a. Google Amicus and the Stored Communications Act**

Google provided an amicus brief in *Chatrie*, which Mr. Brown attaches to his current motion to suppress. *See* 590 F. Supp at 906-07; [*see also* Doc. 1709-6.] Google argued that while the parties focused on the Fourth Amendment, Google’s disclosure of user data was subject to the Stored Communications Act (“SCA”), which generally requires a warrant for disclosure of the contents of electronic communications. [Doc. 1709-6 at 21-22.] Google argued that LH information was subject to the SCA’s warrant requirement because LH information qualified as the contents of electronic communications. [*Id.* at 23.]

**2. *United States v. Davis***

In *Davis*, the district court did wade into standing, but only because the data swept up in the challenged geofence warrant belonged to a third party, and not the defendant. 2022 WL 3009240 at \*8. Accordingly, the court found the defendant lacked standing and denied the motion to suppress. *Id.* It still noted that, if a defendant somehow had a legitimate expectation of privacy in the area searched, the good faith exception would still have applied to avoid exclusion of the evidence collected. *Id.* at \*9.

**3. *United States v. Rhine***

In *Rhine*, a January 6th Capitol riot case, the challenged warrant included a three-step process for seizing data for individuals in and immediately around the Capitol building between 2 and 6:30 p.m. on January 6, 2021. 2023 WL 372044 at \*17-18. At step one, Google was to provide anonymized data; at step two, the government would review this data, including control data to cross-reference; and at step three, the government would return to the court for further approval to identify the devices from which it wanted additional subscriber information based upon information obtained from the earlier steps. *Id.* at \*18. The court denied the defendant's motion to suppress and found that (1) particularized probable cause supported the geofence warrant, and (2) any alleged infirmities fell into the good



faith exception. *Id.* at \*27. It did not reach the issue of whether the defendant had a reasonable expectation of privacy over his location within the Capitol building or over his LH data generally. *Id.* The court did note, however, that it was “far from clear” that defendant’s “Fourth Amendment rights were implicated by the anonymized list provided at step one [of the geofence warrant].” *Id.* at \*28.

#### 4. *United States v. Smith*

In *Smith*, the challenged geofence warrant authorized an hour-long search that covered roughly 98,000 square meters around a post office that had been robbed. 2023 WL 1930747 at \*1, 4. The warrant followed a three-step process, akin to the one in *Rhine*, though law enforcement did not return to the court for further authorization for de-anonymized data at step three. *See id.* at \*4. The court found that the geofence warrant contained sufficiently particularized probable cause, citing the limited time period, the rural area covered, and an affidavit with evidence that the suspect was possibly using a phone. *Id.* at \*8-9. Nevertheless, the court found that law enforcement failed to comply with the warrant by not returning to the court after step two for further authorization to collect de-anonymized data, but despite this, still excused law enforcement’s failing under the good faith exception. *Id.* at \*9-12. The court also declined to resolve the issue of

whether individuals possess a reasonable expectation of privacy in their LH. *Id.* at \*6.

### **5. *United States v. Scott Carpenter***

In *Scott Carpenter*, the challenged geofence warrant sought LH information around the scenes of ten armed robberies and attempted armed robberies, each during 30-minute windows. 2023 WL 3352249 at \*1, 4. Each geographic circle captured the location of a robbery and a roughly half-mile radius around it. *Id.* at \*4. Google provided anonymized LH data for the ten locations, which contained roughly 1,000 email accounts, and then law enforcement asked Google (without additional court approval) to provide identifying data for two of those accounts. *Id.* at \*4. The court found that the good faith exception applied, and therefore, did not address Fourth Amendment standing or the warrant's validity. *Id.* at \*9.

### **6. *United States v. Wright***

In *Wright*, the challenged geofence warrant sought information from five locations for a 4.5-hour period. 2023 WL 5804161, at \*9. The Court rejected an overbreadth argument based on the collection of data from individuals other than the defendant, finding that, to the extent the warrant was overbroad, it did not implicate the defendant's Fourth Amendment rights. *Id.* at \*10. The Court ultimately concluded that the good faith exception applied, noting that a warrant's

failure to satisfy the Fourth Amendment's overbreadth and particularity requirements did not bar applying that exception. *Id.* at \*11.

## **7. State Appellate Decision**

In addition to the federal cases discussed above, at least one state court opinion has addressed geofence warrants in the context of motions to suppress.

### **a. California Second District Court of Appeal**

In *People v. Meza*, two defendants moved to suppress evidence seized from a geofence warrant that sought LH data within six target locations that a murder victim had visited before his death. 90 Cal. App. 5th 520, 527-531 (2023), *reh'g denied* (Apr. 25, 2023), *review filed* (May 22, 2023). The areas searched were acres-wide and located in residential, urban areas. *Id.* at 528-29. The warrant had a three-step process, in which (1) Google provided anonymized data; (2) the government reviewed the data; and (3) law enforcement could demand identifying information from Google for the devices law enforcement deemed relevant. *Id.* at 529-30. The superior court initially denied the motions to suppress, *id.* at 531, but on appeal, although the court determined probable cause supported the warrant, it nevertheless found that it lacked sufficient particularity because it “provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google.” *Id.* at 536-38. The court further

determined that the warrant was overbroad because (1) it authorized the identification of any individual within six large search areas without any particularized probable cause as to each person or their location; and (2) law enforcement failed to draw the location and time boundaries as narrowly as they could have given the available information. *Id.* at 539-40. Ultimately, though, the appeals court affirmed the lower court decision because the good faith exception applied to the warrant. *Id.* at 543-45.

## **B. Magistrate Judge Decisions Re: Geofence Warrants Pre-Issuance**

Finally, in addition to the cases addressing motions to suppress, a few magistrate judge opinions have addressed Fourth Amendment issues pertaining to the denial of geofence warrant applications.

### **1. Northern District of Illinois**

In July 2020, Magistrate Judge M. David Weisman denied a three-step (with no additional judicial oversight) geofence warrant application, which had two proposed geofence locations with 100-meter radiuses in commercial and residential areas. *See Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A*, No. 20-M-297, 2020 WL 5491763, at \*1 (N.D. Ill. July 8, 2020). The court determined the scope of the search was overbroad and that the items to be seized were not particularly described. *Id.* at \*3.

In August 2020, Magistrate Judge Gabriel A. Fuentes denied a revised version of that geofence warrant application, which had narrowed the geographic scope of the geofences, because it still lacked probable cause and was still not sufficiently particular. *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 733-34, 753-54, 757 (N.D. Ill. 2020). The government proposed a two-stage process in which it would receive only anonymized data. *Id.* at 747. After prompting from the court, the government later explained that, once it had the anonymized list of device IDs, it could obtain the subscriber information via subpoena and without further aid of a search warrant. *Id.* Based upon this, the court saw “no practical difference between a warrant that harnesses the technology of a geofence . . . to generate a list of device IDs that the government may easily use to learn the subscriber identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities.” *Id.* at 749. Despite denying the warrant application, the court did not reach the open question of the privacy interest in LH data because the government “treated its proposed geofences as a search.” *Id.* at 740.

In October 2020, Magistrate Judge Sunil R. Harjani found that a different proposed geofence warrant satisfied the Fourth Amendment’s requirements. *See Matter of Search Warrant Application for Geofence Location Data Stored at*

*Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 364 (N.D. Ill. 2020). The two-step warrant (without additional judicial review) outlined six target locations that law enforcement identified as connected to a series of arsons. *Id.* at 351. The court found that the government structured the target locations to “minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses.” *Id.* at 353. Specifically, the court noted that the warrant was limited both (1) in time, with 15-30-minute time frames for each target location, and (2) in location, circling the arson crime scenes, which were mostly commercial parking lots where “there [w]as a fair probability that the location data of perpetrators, co-conspirators and witnesses to the incidents will be uncovered.” *Id.* at 357-58. As with prior opinions, the court did not reach the issue of whether a warrant was necessary to request Google LH data. *Id.* at 359.

## **2. District of Kansas**

In June 2021, Magistrate Judge Angel D. Mitchell denied a geofence warrant application because it did not establish probable cause that evidence of the crime would be located in Google’s records. *Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1156 (D. Kan. 2021). The court noted that the affidavit did not suggest that any relevant perpetrator or

witness had a smartphone, nor did it address the anticipated number of individuals likely to be encompassed within the targeted data. *Id.* at 1157. Further, the court found that the warrant was not sufficiently particularized because the geofence boundary encompassed two public streets and because it sought data within the geofence's margin of error, which could return data outside the geofence where there were residences and businesses. *Id.* at 1158. The court also determined that the requested time frame was not sufficiently tailored as the government failed to explain the reasoning behind choosing its particular temporal window. *Id.*

### **3. D.C. District**

In December 2021, Magistrate Judge G. Michael Harvey granted a three-step (with judicial oversight after step two) geofence warrant application that sought LH information for devices in an area of roughly 875 square meters, during segments of time ranging from 2 to 27 minutes, on 8 specified dates, totaling 185 minutes overall. *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 72-74, 91 (D.D.C. 2021). The government represented that the data it requested corresponded with criminal activity caught on surveillance footage, which also showed suspects using cell phones. *Id.* at 72. The court found sufficient probable cause and particularity, noting that the multi-stage process “ameliorates possible overbreadth concerns” because even “if third-party devices

appear within the government's requested geofence, those persons' location information will be anonymized at step one" before being filtered out at step two. *Id.* at 79-90.

#### 4. Southern District of Texas

In February 2023, Magistrate Judge Mitchel Neurock issued a public order that largely mirrored an earlier, sealed grant of a step one geofence warrant. *Matter of Search of Info. Stored at Premises Controlled By Google*, No. 2:22-MJ-01325, 2023 WL 2236493, at \*1 (S.D. Tex. Feb. 14, 2023).<sup>8</sup> The warrant sought LH information for an area surrounding a business where unauthorized bank withdrawals took place on nine separate occasions, with requested time periods ranging from 5 to 17 minutes each. *Id.* at 1-3, 6. The warrant sought only anonymized data, and law enforcement would have to return to the court with subsequent warrant requests to unmask devices identified in step one. *Id.* at 6. The court noted that it was questionable whether a warrant was even required in a step one situation, or if the limited nature of the anonymized LH information fit within the third-party doctrine. *Id.* at 7-8. Regardless, the court found (1) probable cause

---

<sup>8</sup> The public order is largely identical to the original sealed version, with "redactions and minor wording changes" to protect the underlying investigation, but "no factual changes." *Matter of Search of Info. Stored at Premises Controlled By Google*, 2023 WL 2236493, at \*1, n.1.



that a crime was committed and that evidence would be found on Google's servers; (2) the request was sufficiently particular given the detailed description of the target area; and (3) the request was not overbroad because the geographic area and time periods closely tracked the probable cause to justify the disclosure of the anonymized data with a minimized likelihood that it would sweep up identifiable data of uninvolved individuals. *Id.* at 9-14.

With this context, the undersigned now turns to the search warrants at issue in this case.

## **II. THE CHALLENGED WARRANTS**

### **A. Search Warrant 1:19-MC-1550**

On September 26, 2019, FBI Special Agent ("SA") Jason Cleary submitted an affidavit in support of geofence warrant 1:19-MC-1550 (the "First Warrant"), which sought to search for "information associated with cellular devices that reported a device location within a particularly defined geographical region between 9:35 pm and 9:56 pm (EST) on November 22, 2014 that [was] in the custody and control of Google." [Doc. 1709-1.] SA Cleary stated that Google could determine which mobile devices were in a particular geographic area during a particular time frame based on location data collected during the use of various Google products. [*Id.* at. 8.] He submitted that such information could inculpate

or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation. [*Id.*] Further, SA Cleary stated that the Google account subscriber information “may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users” and that “even if subscribers insert false information to conceal their identity, this information often can provide clues to their identity, location, or illicit activities.” [*Id.*]

In his affidavit, SA Cleary stated the following: the FBI was investigating NTG for illegal activity, including racketeering, racketeering conspiracy, drug trafficking, and crimes of violence; on November 22, 2014, NTG member Dontavis Davis was killed during a failed robbery attempt; according to a cooperating witness, Mr. Brown sent multiple crews of NTG members throughout the Atlanta area to retaliate against rival gang members, who were rumored to have been responsible for the killing; the same day, November 22, Atlanta police were notified of a shooting in the vicinity of 1029 McDaniel Street, Atlanta, GA, and found the body of Demetrius Davis next to the JVC grocery store at that address; surveillance video showed five vehicles turning right off McDaniel Street at roughly 9:40 p.m. and park at the grocery store; multiple people got out of the vehicles and a camera captured an individual, later identified as Mr. Brown, taking

a rifle out of a sedan, running toward the victim, and then backing up into frame and shooting the rifle multiple times; the vehicles were seen driving away at roughly 9:44 p.m.; and a 911 call was placed at 9:56 p.m. and Atlanta police arrived at the scene at 9:59 p.m. [Doc. 1709-1 at 9-11.]

SA Cleary affirmed that there was probable cause to search information in the possession of Google to determine which devices were in the Target Location, which was a “geographic area covering the area where [the murder victim’s] body was found and where the five vehicles were parked on November 22, 2014.” [Doc. 1709-1 at 12.] The First Warrant described the Target Location as a “polygon defined by ... four latitude/longitude coordinates connected by straight lines.” [*Id.* at 15.] In total, the area was roughly 20 by 55 yards. [See Doc. 1730-1.] The material to be searched was described as follows:

- (1) location history data, sourced from methods including GPS, wi-fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google accounts associated with the responsive location history data.

[Doc. 1709-1 at 15.]

SA Cleary’s affidavit stated that, in “order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates

that Google will disclose the information to the government in stages rather than disclose all of the information for which the government has established probable cause to search at once.” [Doc. 1709-1 at 13.] The First Warrant explained this process as follows:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A.
2. For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the “Anonymized List”).
3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.
4. Google is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google account associated with each device ID about which the government inquires.

[*Id.* at 16.] The First Warrant then provided that the information to be seized was all information that constituted “evidence of violations of 18 U.S.C. §§ 1962 and 1959 . . . on November 22, 2014 involving known and unknown person(s).” [*Id.*]

United States Magistrate Judge Justin S. Anand signed the First Warrant, finding that the affidavit established probable cause to search for and seize the information in the custody or control of Google associated with cellular devices

that reported a device location within the geofence area between 9:35 p.m. and 9:56 p.m. (EST) on November 22, 2014. [Doc. 1709-1 at 17.] On November 14, 2019, Google provided the initial anonymized results, which consisted of four accounts. [Doc. 1709-3 at 12.] SA Cleary then requested that Google provide the device identification and subsequent user information for each of those accounts, which Google provided on December 24, 2019. [*Id.*] This information included the email account pistolplay31@gmail.com with the recovery email Terrybrownjr5@yahoo.com and Google Account ID 1010160635412. [Doc. 1709-2 at 12.]

**B. Search Warrant 1:20-MC-152**

On January 29, 2020, SA Cleary submitted an affidavit in support of search warrant 1:20-MC-152 (the “Second Warrant”), which sought a search of “[i]nformation associated with the email address pistolplay31@gmail.com and Google Account ID 1010160635412 that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at Mountain View, CA.” [Doc. 1709-2 at 2.] The affidavit explained that these accounts were identified during the execution of the First Warrant. [*Id.* at 12.] The Second Warrant sought information, including location data, from Google for these accounts for four time periods: August 10, 2013 from 10 p.m. to August 11 at 3

a.m.; September 30, 2014 from 6 p.m. to 10 p.m.; October 16, 2014 from 6 p.m. to October 17 at 6 a.m.; and November 22, 2014 from 12 p.m. to November 25 at 12 p.m. [*Id.* at 29-30.] The supporting affidavit explained that Mr. Brown was implicated in shootings during these time periods. [Doc. 1709-2 at 7-15.] United States Magistrate Judge Catherine Salinas signed the Second Warrant, finding that the affidavit established probable cause to search for and seize the aforementioned information associated with the accounts. [*Id.* at 33.]

### **C. Search Warrant 1:20-MC-364**

On February 28, 2020, SA Cleary submitted an affidavit in support of search warrant 1:20-mc-364 (the “Third Warrant”), which sought a search of “[i]nformation associated with cellular devices that reported a device location within a particularly defined geographical region between 9:50 pm and 9:56 pm (EST) on November 22, 2014 that [was] in the custody or control of Google.” [Doc. 1709-3.] In this warrant, the FBI requested a “larger geographic area [that] may provide information related to the co-conspirators” involved in the events of November 22, 2014. [*Id.* at 13.] The Target Location was the geographic area surrounding the area where Davis’s body was found and where the five vehicles were parked on November 22, 2014. [*Id.* at 14.] United States Magistrate Judge Christopher C. Bly signed the Third Warrant, finding that the affidavit established

probable cause to search for and seize the information that was in the custody or control of Google and that was associated with cellular devices that reported a device location within the geofence area between 9:50 p.m. and 9:56 p.m. (EST) on November 22, 2014. [*Id.* at 20.]

### **III. DISCUSSION**

Mr. Brown moves the Court to suppress the evidence from the First, Second, and Third Warrants because the associated searches and seizures violated his rights under the Fourth Amendment. [Doc. 1709 at 1.] Mr. Brown argues that (1) the warrants are impermissible general warrants; (2) the First Warrant lacks requisite particularity and probable cause; and (3) the Second and Third Warrants are based upon the findings of the First Warrant and are therefore the poisonous fruits of the First Warrant. [*Id.* at 4-6.] Mr. Brown also requests an evidentiary hearing. [*Id.* at 11.] The Court takes up its analysis of Mr. Brown's arguments below.

#### **A. Analysis**

##### **1. Fourth Amendment Standing**

Mr. Brown first contends that the FBI's acquisition of his Google LH data was a search and seizure under the Fourth Amendment because he had a reasonable expectation of privacy in that data. [Doc. 1709 at 30-38.] He argues that Google LH data—with its high degree of precision and retrospective quality—reveals the

privacies of a person's life that are protected by the Fourth Amendment. [*Id.* at 33-38.] Next, he asserts the third-party doctrine does not apply because Google LH is different from third-party business records, given its exhaustive nature and the fact that users do not voluntarily share that information with Google in "any meaningful sense." [*Id.* at 38-43.] Additionally, Mr. Brown argues that he had a property interest in his LH data that belongs to himself, but not Google. [*Id.* at 43-46.] Essentially, he asserts that his LH data was held in trust by Google, making it a bailee with a duty to him, and urges that he retained the right to exclude others from accessing his LH data. [*Id.* at 45.] The government, meanwhile, argues in response that Mr. Brown had no protected Fourth Amendment interest in any of the information disclosed pursuant to the geofence warrants. [Doc. 1730 at 9-18.]

An individual has a legitimate expectation of privacy in the object of a search where he has (1) a subjective expectation of privacy in the object of the challenged search, and (2) society is prepared to recognize that expectation as legitimate. *See United States v. Cohen*, 38 F.4th 1364, 1368 (11th Cir. 2022). No "single rubric definitively resolves which expectations of privacy are entitled to protection," but there are "basic guideposts." *Carpenter*, 138 S. Ct. at 2213-14. These guideposts include securing the privacies of life against arbitrary power and placing "obstacles in the way of a too permeating police surveillance." *Id.* at 2214 (quoting *United*



*States v. Di Re*, 332 U.S. 581, 595 (1948)). What constitutes a legitimate expectation of privacy is complicated by “[d]ramatic technological change” that “may lead to periods in which popular expectations are in flux.” *United States v. Jones*, 565 U.S. 400, 427 (2012) (Alito, J., concurring). As Justice Alito noted, “even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.” *Id.*

Accordingly, changing technology has spurred new Fourth Amendment considerations. In *Katz v. United States*, the Supreme Court determined that the Fourth Amendment protects “people, not places” and, in turn, held that surveillance of a private conversation in a public phone booth was a search within the meaning of the Fourth Amendment that would require judicial oversight. 389 U.S. 347, 351-53 (1967) (“To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”). In *United States v. Jones*, the Court decided a GPS tracking case on physical trespass grounds, concluding that attaching such a device to a car is a search within the meaning of the Fourth Amendment because of the physical trespass onto the car. 565 U.S. at 404-05. But five Justices also agreed that, even if there were no physical trespass, privacy concerns were still raised by such GPS tracking. *Id.* at 415-16 (Sotomayor,

J., concurring); *id.* at 426 (Alito, J., concurring). Finally, in *Riley v. California*, the Court held the search incident-to-arrest exception<sup>9</sup> was generally inapplicable to cell phones, noting the vast quantity of private data they hold, including “[h]istoric location information” that “can reconstruct someone’s specific movements.” 573 U.S. 373, 395-96 (2014).

With the backdrop of these cases, the Supreme Court held in *Carpenter v. United States* that the government “conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user’s past movements” because “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through” cell-site location information (“CSLI”).<sup>10</sup> 138 S. Ct. at 2211, 2217. The Court determined that the fact that the CSLI was held by a third-party

---

<sup>9</sup> This exception to the warrant requirement allows law enforcement to conduct a warrantless search of an individual who is legally arrested. *Riley*, 573 U.S. at 382.

<sup>10</sup> CSLI is composed of time-stamped records generated when a phone connects to a cell site, which are usually mounted on an antenna tower. *Carpenter*, 138 S. Ct. at 2211. Unlike GPS data, or the LH information at issue in this case, “the precision of [CSLI] depends on the size of the geographic area covered by the cell site.” *Id.*

did not “by itself overcome the user’s claim to Fourth Amendment protection.”<sup>11</sup> *Id.* at 2217. The Court concluded that historical cell-site records “present even greater privacy concerns than the GPS monitoring of a vehicle” because a cell phone tracks “nearly exactly the movements of its owner.” *Id.* at 2218. The Court explained that individuals “compulsively carry cell phones with them” and cell phones follow an owner “beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Id.* It further distinguished retrospective CSLI from GPS tracking because “police need not even know in advance whether they want to follow a particular individual, or when.” *Id.*

Here, akin to the CSLI in *Carpenter*, LH information “does not fit neatly under existing precedents.” 138 S. Ct. at 2214. Based on the aforementioned cases, though, the undersigned is skeptical that either step of the First Warrant—receiving the anonymized data or obtaining deanonymized data after review of the anonymized data—is actually a search within the meaning of the Fourth Amendment. As to the first step, the anonymized data dump does not seem to implicate the Fourth Amendment because it is doubtful a person has a reasonable

---

<sup>11</sup> “Ordinarily, a person lacks a reasonable expectation of privacy in information he has voluntarily disclosed to a third party.” *United States v. Trader*, 981 F.3d 961, 967 (11th Cir. 2020).

expectation of privacy over information that cannot be connected to him. *See Rhine*, 2023 WL 372044, at \*28. As to the second step, the deanonymized data is composed of information that the government can request via administrative subpoena under 18 U.S.C. § 2703(c). *See* 18 U.S.C. § 2703(c)(2); *see also United States v. Jenkins*, No. 1:18-CR-181-MLB-CMS, 2019 WL 2482171, at \*2 (N.D. Ga. Feb. 5, 2019), *report and recommendation adopted*, 2019 WL 1568154 (N.D. Ga. Apr. 11, 2019) (concluding that *Carpenter* did not change the application of § 2703).

Of course, the combination of the two steps allows law enforcement to link a person's Google account to a specific location at a specific time, which may offend notions of privacy. Even so, flattening these two steps into one step—as the First Warrant essentially did—does not seem to present the kind of privacy concerns that the Supreme Court has guarded against. Unlike in *Katz*, law enforcement did not seek, nor did they receive, any surveillance of a private conversation. There was no physical trespass beyond public spaces like the GPS tracking in *Jones*. And importantly, the present warrant essentially took a “snapshot” of phone users' LH information within a specific, public place (less than half the size of a football field), for a limited period of time (less than half an hour), and therefore it could not provide a “comprehensive chronicle” of a user's

movements, as was the Court’s concern in *Riley* and *Carpenter*. *See also United States v. Manning*, No. 1:19-CR-00376-TWT-RGV, 2021 WL 5236660, at \*6 (N.D. Ga. Aug. 20, 2021), *report and recommendation adopted sub nom. United States v. Sterling*, 2021 WL 5280567 (N.D. Ga. Nov. 12, 2021) (collecting cases for the proposition that cell tower dumps do not present the Fourth Amendment concerns present in *Carpenter*). As a result, the data provided in response to the First Warrant was information akin to that of surveillance video—showing the location of individuals in a specific, tightly enclosed area—which does not typically implicate the Fourth Amendment.

To be sure, the use of geofence warrants will continue to test constitutional boundaries, and if the location or temporal window of a particular geofence warrant (or series of warrants) expands too far, that warrant would undoubtedly provide a defendant with Fourth Amendment standing.<sup>12</sup> If, for instance, law enforcement used a series of geofence warrants to track an individual’s LH over an extended period of time, *Carpenter* would almost certainly be implicated. In any case,

---

<sup>12</sup> Other courts have echoed this sentiment. *See Rhine*, 2023 WL 372044, at \*28 n.22 (“[T]he Court acknowledges that the scope of legally obtainable anonymous data made possible by geofencing technology could present potentially significant risks to privacy, even if those privacy interests cannot be expressed through Defendant’s challenge to step one of this particular warrant, on these particular facts, under current law.”).

Google's massive LH data trove is a dramatic technological development, and it remains unclear the extent to which society is prepared to recognize an expectation of privacy in that data. Accordingly, as other courts have pointed out, legislation regarding LH data may be necessary to better define the outer bounds of society's expectations of privacy. *See Chatrue*, 590 F. Supp. 3d at 926 ("At base, these matters are best left to legislatures . . . . This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data."). Of course, the SCA indicates that an individual has a privacy interest in LH data, as Google has pointed to, but it is not yet settled if LH information is actually an electronic communication covered under that Act.

In sum, the undersigned is of the view that the Fourth Amendment is likely not infringed by the acquisition of LH information through the use of a geofence that is as temporally and geographically restricted as the one in the First Warrant was; however, I am not prepared to conclude that the acquisition of LH information never implicates the Fourth Amendment. Ultimately, as other courts faced with geofence warrants have found, there is no need to decide the question of whether Mr. Brown had a reasonable expectation of privacy over his LH data. That is so because the government did in fact obtain a warrant that, as will be discussed presently, was supported by probable cause and sufficiently particularized; and

regardless of any infirmities to that warrant, it still would fall into the good faith exception to the exclusionary rule, such that suppression is unwarranted.<sup>13</sup>

## 2. Probable Cause

Mr. Brown argues that the First Warrant, and the subsequent warrants, lacked probable cause to (1) justify a search of 600 million Google accounts who had location history enabled; and (2) obtain his personally identifying Google LH information during “step two of the warrant.” [Doc. 1709 at 46-48.] Mr. Brown argues that the FBI “had no information to distinguish among” the four anonymized accounts in step one and, ostensibly, ignored probable cause considerations when it went back to Google for the deanonymized information for all four. [*Id.* at 47.]

Establishing probable cause “is not a high bar” and instead “requires only the kind of fair probability on which reasonable and prudent people, not legal technicians, act.” *Kaley v. United States*, 571 U.S. 320, 338 (2014) (internal quotations omitted) (cleaned up). The task of the issuing judge is “simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence

---

<sup>13</sup> This line of reasoning also applies to Mr. Brown’s property interest argument, which is compelling in the sense that it avoids the murky waters of a reasonable expectation of privacy analysis. But even assuming that a person’s LH data could qualify as his papers or effects that are afforded Fourth Amendment protection, the good faith exception applies, as analyzed below.

of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). When reviewing a search warrant after the fact, the Court will uphold the determination of the issuing judge so long as he had a “substantial basis” for concluding that probable cause existed. *Id.*; *United States v. Joseph*, 709 F.3d 1082, 1093 (11th Cir. 2013), *overruled on other grounds by Ruan v. United States*, 142 S. Ct. 2370, 2376 (2022).

As an initial matter, Mr. Brown’s first argument that the First Warrant lacked probable cause to justify a search of 600 million Google accounts is based on an incorrect premise. As explained in *Rhine*, “the relevant question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize.” 2023 WL 372044 at \*28. Here, the First Warrant did not authorize the government to search and seize 600 million accounts that had LH turned on for data within the geofence, but rather authorized the government to obtain from Google LH information about users in a small geographic area during a specific window of time, both of which were directly linked to a murder. There is nothing in the record to suggest that the government searched all of Google’s 600 million user accounts—instead Google simply ran a search of its database in response to the warrant in order to provide the specific information requested. As the court in *Rhine* explained, under the theory that the First Warrant was overbroad because it



allowed Google to conduct such a search, “no doubt many search warrants and most third-party subpoenas for protected records would be unconstitutionally overboard because they necessarily would require the third party to search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server.” *Id.*<sup>14</sup> Accordingly, the undersigned will not find the First Warrant overbroad simply because Google maintains a vast database of user information.

Next, Mr. Brown’s second argument appears to assume that to be constitutionally sound, a geofence warrant needs a multi-step process<sup>15</sup> wherein the government must receive additional court approval to obtain deanonymized data. Mr. Brown cites Magistrate Judge Harvey’s December 2021 order granting a geofence warrant for this proposition. [*See* Doc. 1709 at 48.] But that order also

---

<sup>14</sup> Though not explicitly stated, Mr. Brown’s first argument appears to be a breadth challenge. *United States v. Lebowitz*, 647 F. Supp. 2d 1336, 1351 (N.D. Ga. 2009), *aff’d*, 676 F.3d 1000 (11th Cir. 2012) (explaining that breadth “deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based”). As discussed, it is clear that the warrant was not overbroad given the parameters of what the government requested. Further, as discussed in *Wright*, to the extent that the First Warrant was overbroad, Mr. Brown lacks Fourth Amendment standing to challenge the collection of data from third parties. *See Wright*, 2023 WL 5804161, at \*10.

<sup>15</sup> To be clear, the First Warrant did lay out a multi-step process, but it appears created for practical reasons like data management—not to require an additional probable cause assessment.

notes that such a process may not be required “where the duration and location of the government’s proposed geofence and nature of the crime under investigation effectively means that *almost all* location data retrieved will be for individuals who are either the perpetrators, co-conspirators, or witnesses to the crime.” 579 F. Supp. 3d at 88 n.24. Such was the situation here. The geofence was so tightly drawn—including an area of no more than 50 yards beyond the murder site for a period of less than 30 minutes late in the evening—that it was reasonable to conclude that almost all LH information collected would be for those directly involved in or, at least in view of, the criminal activity.

In sum, the magistrate judge in this case had a substantial basis for concluding that probable cause existed to retrieve *all* the LH data within the geofence. In the simplest terms, the affidavit established that Mr. Brown had been identified on surveillance video using a rifle at the scene of the murder in the minutes before Atlanta police arrived and found the victim. [Doc. 1709-1 at 9-11.] It further established that surveillance video showed five cars, carrying at least 15 people, parked at the scene of the murder that also drove off after the shooting. [*Id.*] It explained that Mr. Brown was part of a gang under investigation for racketeering, drug trafficking, and crimes of violence, and that the shooting was part of a coordinated effort to retaliate against another gang. [*Id.*] The affidavit

also explained how Google LH is created, what LH and subscriber information could be captured, and how such information could be used in the criminal investigation. [*Id.* at 8-9.] Accordingly, it is clear that the affidavit gave the magistrate judge a substantial basis to conclude that there was a fair probability that Google possessed evidence related to the crimes being investigated.<sup>16</sup>

And finally, although Mr. Brown does not advance this argument, the Court observes that the affidavit did not connect cell phone use to the crime scene or the criminal activity, which may have better supported a probable cause determination. *See Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 72 (noting that surveillance showed suspects using cell phones when engaged in the criminal activity that the proposed geofence would be used to investigate). Regardless, it is a matter of common sense that cell phones would likely have been present at the crime scene or used in the coordination efforts for the alleged criminal activities that day. *See Riley v. California*, 573 U.S. 373, 385 (2014) (“[C]ell phones . . . are now such a pervasive and insistent part of daily life

---

<sup>16</sup> As the government correctly points out, investigators could use the LH information to “reconstruct what took place at the crime scene at the time of the crime, “identify the shooter and any accomplices,” “identify potential witnesses and obtain further evidence,” “corroborate and explain other evidence, including surveillance video and witness testimony, and “rebut potential defenses.” [Doc. 1730 at 20.]

that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”); *see also United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021), *cert. denied*, 142 S. Ct. 1352 (2022) (concluding that probable cause supported a warrant for cell tower data in a robbery case even though there was no direct evidence that the suspected robber had a cell phone because “judges were not required to check their common sense at the door and ignore the fact that most people ‘compulsively carry cell phones with them all the time’”).

### 3. Particularity

Next, Mr. Brown argues that the First Warrant (as well as the later warrants) violated the particularity requirement because it did not specify the specific accounts to be searched and data to be seized. [Doc. 1709 at 48-52.] Mr. Brown asserts that, because the warrant did not follow “the typical three-step process in geofence warrants, and skipped the typical second step, the warrant left it up to Google and the FBI to decide which users would have their de-anonymized personally identifying account information handed over to the FBI.” [*Id.* at 50.]

The Fourth Amendment requires that a warrant “particularly describe[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “This particularity requirement exists ‘to protect individuals from being subjected to general, exploratory searches.’” *United States v. Moon*, 33 F.4th 1284,

1296 (11th Cir.), *cert. denied*, 143 S. Ct. 376 (2022) (quoting *United States v. Khanani*, 502 F.3d 1281, 1289 (11th Cir. 2007)).

As discussed in the probable cause section above, the warrants did not authorize the search and seizure of information from all 600 million Google user accounts, as Mr. Brown suggests. Instead, the First Warrant sufficiently and particularly described the information for Google to retrieve: (1) LH data generated from devices that reported a device location within an area roughly 20 by 55 yards between 9:35 p.m. and 9:56 p.m. on November 22, 2014, and (2) identifying information for Google accounts associated with the responsive LH data. [See Doc. 1730-1.] The particularity in the First Warrant thus aligns with the parameters discussed in other geofence cases, given the geofence's limited area and time frame. *See Smith*, 2023 WL 1930747 at \*8-9 (finding sufficient particularity for geofence that covered roughly 98,000 square meters in rural area for an hour-long period); *Rhine*, 2023 WL 372044 at \*17-18, 27 (finding particularized probable cause in three-step geofence warrant that encircled the Capitol for four-and-a-half hours on January 6, 2021); *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 357-59 (finding sufficient particularity where geofences were limited to 15-30 minute time frames and surrounded six locations, which were mostly

commercial car lots, connected to a series of arsons). And it was not nearly as expansive as the geofence warrants that other courts have expressed concern about. *Chatrie*, 590 F. Supp. 3d at 918-19, 929-30 (finding insufficient particularized probable cause where geofence warrant included 300-meters in an urban environment and sought information outside the geofence, without geographic restriction, from users who had been identified within the geofence); *Meza*, 90 Cal. App. 5th at 539-40 (finding insufficient particularity where geofence included six large areas and law enforcement failed to draw the location and time boundaries as narrowly as they could have).

As such, in no way did the First Warrant authorize a general rummage through all of Mr. Brown's data or through all of the data of Google's users by the government. And the mere fact that Google had to look at a silo of data does not make the First Warrant unconstitutional or insufficiently particularized. There is no requirement that geofences follow any specific three-step process, though it may be necessary to do so in certain situations where vast amounts of data from multiple areas is being collected. But as already discussed, the magistrate judge in this case found that probable cause supported the retrieval of LH data, and corresponding subscriber information, from *all* devices within a relatively small area for a short period of time. Accordingly, it met the Fourth Amendment's particularity

requirements, and there was no need for investigators to return for court approval to receive the deanonymized data.

#### **4. Reliance on Racketeering Activity**

Mr. Brown also argues that the warrants were impermissibly general because they allowed law enforcement to search and seize evidence of violations of 18 U.S.C. §§ 1959 and 1962, which prohibit “racketeering activity,” and therefore encompass dozens of federal crimes. [Doc. 1709 at 20-24.] Based on this, Mr. Brown argues that the warrants were not sufficiently particularized. [*Id.* at 27.]

As Mr. Brown acknowledges, the Eleventh Circuit has upheld warrants that tie searches to specific statutory violations. *See United States v. Majors*, 196 F.3d 1206, 1216 (11th Cir. 1999) (concluding that a warrant was sufficiently particular that allowed for the search of evidence in violation of 18 U.S.C. §§ 1341 and 1342). And this Court has upheld warrants that authorized the seizure of evidence of crimes that were encompassed in this case’s investigation. *See United States v. Capote*, No. 1:15-CR-00338-MHC-CMS, 2016 WL 11650552, \*2-3 (N.D. Ga. May 5, 2016) (finding warrant was sufficiently particular that provided for the seizure of evidence tied to mail and wire fraud). Regardless, as discussed above, the First Warrant did not give investigators broad authority to search for all evidence of the subject offenses without any limitation. Instead, it allowed only

for the disclosure of identifying information, as provided in 18 U.S.C. § 2703(c)(2), for the Google accounts associated with each device within the warrant's very limited geofence. Accordingly, the warrants satisfied the Fourth Amendment's particularity requirement. Even assuming, though, that the First Warrant, and the subsequent two additional warrants, were not supported by sufficiently particularized probable cause, suppression is not the appropriate remedy, for the reasons explained immediately below.

### **5. Good Faith Exception**

The exclusionary rule acts as a remedy to unconstitutional searches by prohibiting the government from using evidence seized as a result of an illegal search in a subsequent criminal prosecution. *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002). But evidence “obtained in objectively reasonable reliance on a subsequently invalidated search warrant” is generally not subject to the exclusionary rule. *Leon*, 468 U.S.C. at 922-23. Suppression is an appropriate remedy, however, where (1) the issuing magistrate judge was “misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth”; (2) the issuing magistrate judge wholly abandoned his judicial role; (3) the warrant was based on an affidavit so devoid of probable cause as to render official belief in its existence entirely



unreasonable; or (4) the warrant was so facially deficient that the executing officers could not presume it to be valid. *Id.* at 923.

Here, even if the First Warrant, and therefore the subsequent warrants, were defective in some way, the good faith exception applies. First, there is no indication that the affidavits upon which the warrants relied were somehow false. Second, there is no suggestion that the issuing magistrate judges abandoned their judicial role. Third, the affidavits were not so devoid of probable cause to render belief in its existence unreasonable. Fourth, the warrants were not so deficient that investigators should have presumed they were invalid. In fact, as described in the analysis above, the First Warrant (1) was supported by a detailed affidavit that provided probable cause, and (2) described in detail the information sought within a time- and area-limited geofence. Additionally, this is a cutting-edge area of the law, which lends further credence to the conclusion that investigators reasonably relied on the challenged warrants.

## **6. Second and Third Warrants**

Mr. Brown challenges the subsequent warrants on the same grounds as the First Warrant. [Doc. 1709 at 17 n.3.] Because the First Warrant is valid, or at least

falls under the good faith exception, the subsequent warrants, which mirror and are derived from the First Warrant, also fall under the good faith exception.<sup>17</sup>

## 7. Evidentiary Hearing

Mr. Brown requests an evidentiary hearing, so the Court may understand the typical three-step geofence warrant process, how the First Warrant skips a step in a way that implicates the Fourth Amendment, and how the Second and Third Warrants are the tainted fruits of the First Warrant. [Doc. 1709 at 11.] No such hearing is necessary. The Court has been able to fully consider the parties' positions through their briefs and assess the state of geofence law through independent research. *See United States v. Booker*, No. 1:11-CR-255-1-TWT, 2013 WL 2903562, at \*2 n.5 (N.D. Ga. June 13, 2013) (noting the Court's broad discretion to hold an evidentiary hearing and explaining such a hearing is required only where factual issues are raised).

## IV. CONCLUSION

For the foregoing reasons, it is **RECOMMENDED** that Defendant's "Motion to Suppress Evidence from Warrants and Request for Evidentiary Hearing" [Doc.

---

<sup>17</sup> Notably, Mr. Brown does not make arguments regarding the specific contents of the subsequent warrants. [See Doc. 1709 at 20 n.3 (explaining that for "the sake of simplicity and to avoid redundancy," Mr. Brown's section on general warrants focused on the First Warrant but that he was challenged the subsequent warrants "on the same grounds").]

1709] be **DENIED**. It is **FURTHER RECOMMENDED** that Defendant's Preliminary Motion to Suppress Evidence [Doc. 1707] be **DENIED AS MOOT**. The government's motion to withdraw its opposition to the motion to suppress evidence [Doc. 1754] is **GRANTED**.

The Court has now ruled on all of this Defendant's pretrial motions. As a result, this case is **CERTIFIED READY FOR TRIAL**.

SO ORDERED and RECOMMENDED this 19th day of September, 2023.

  
\_\_\_\_\_  
JOHN K. LARKINS III  
United States Magistrate Judge