

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

UNITED STATES OF AMERICA,

v.

TERRY BROWN,

Defendant.

:
:
:
:
:
:
:
:
:
:

CRIMINAL ACTION NO.
1:16-CR-427-AT-JKL-31

ORDER

This matter comes before the Court upon review of the Magistrate Judge's Order and Final Report and Recommendation ("R&R") [Doc. 1755], recommending that Defendant's Preliminary Motion to Suppress [Doc. 1707] be denied as moot, and that Defendant's Motion to Suppress and Motion for Evidentiary Hearing [Doc. 1709] be denied. Defendant has filed objections to the R&R. [Doc. 1760].

For the reasons that follow, the Court **ADOPTS** the R&R **in part**, **SUSTAINS** the objections **in part** and **OVERRULES** them **in part**, **DENIES** Defendant's Preliminary Motion to Suppress **AS MOOT**, **DENIES** Defendant's Motion to Suppress pursuant to the good-faith doctrine, and **DENIES** Defendant's Motion for Evidentiary Hearing.

I. Background

Defendant Terry Brown stands accused in this action of one overarching count of RICO¹ Conspiracy, one count of VICAR² murder, and one count of causing the death of a person through use of a firearm in violation of 18 U.S.C. § 924(c). (Second Superseding Indictment, Doc. 1158 at 13, 18-19, 43-45). The charges against Mr. Brown stem from the Government's allegations that Mr. Brown was associated with and engaged in the activities of the Nine Trey Gangsters ("NTG"), a regional Southeastern set of the larger United Blood Nation gang. (Second Superseding Indictment, Doc. 1158 at 13-15). As relevant to the motions at hand, the Government contends that, in furtherance of the gang's racketeering conspiracy, Mr. Brown shot and killed purported rival gang member Demetrius Davis in November 2014. (*Id.* at 19, 43-45).

Thirty-two Defendants in total have been indicted over the life of this criminal RICO case, beginning with the indictment of a single defendant in December 2016. (Doc. 1). Mr. Brown was first named as a Defendant in the Government's Second Superseding Indictment on February 19, 2020 (Doc. 1158), and he is one of only two remaining Defendants awaiting trial. Mr. Brown is slated to face trial on the charges against him on July 29, 2025. (*See* Doc. 1882).

¹ "RICO" is short for the Racketeer Influenced and Corrupt Organizations Act, codified at 18 U.S.C. §§ 1961 *et seq.*

² "VICAR" is short for the Violent Crimes in Aid of Racketeering Activity statute, codified at 18 U.S.C. § 1959.

Before the trial commences, the Court must resolve Mr. Brown's pending Motion to Suppress, which implicates the Fourth Amendment issue of geofence warrants and which, if granted, would eliminate key evidence the Government intends to use to prove its case. Specifically, Mr. Brown seeks to suppress the evidence obtained by the Government pursuant to three warrants, the first of which, dated September 26, 2019, allowed the FBI to collect the location history data of all Google users within a 20-by-50-meter area during a 21-minute period (i.e., a "geofence") corresponding to the location and time frame of the murder of Demetrius Davis on November 22, 2014. This first geofence warrant revealed that a device associated with Mr. Brown's Google account was present within the geofence at 9:52:50 p.m. on the date of the murder. [Doc. 1709 at 10]. In a second warrant application dated January 29, 2020 -- which was not a geofence warrant -- the FBI sought to obtain from Google Mr. Brown's particular location history data from four different time periods corresponding to four different crimes (including, as relevant to the Davis murder, the 72-hour period of November 22, 2014 at 12:00 noon to November 25, 2014 at 12:00 noon) without any prescribed geographical bounds. A month later on February 28, 2020, the FBI applied for and received a third warrant, seeking Google location history data from a larger geographic area surrounding the Davis murder in an effort to obtain information about co-conspirators who were present.

To provide context for the warrants at issue in this case, some exposition of Demetrius Davis's murder is necessary. According to the Government, the Atlanta

Police Department (“APD”) responded just before 10 p.m. on November 22, 2014 to reports of a shooting next to a grocery store. (First Search Warrant Application (“First Warrant”), Doc. 1709-1 at 10.)³ Demetrius Davis was found dead with multiple gunshot wounds at the scene. (*Id.*). APD gathered surveillance footage from multiple security cameras belonging to the grocery store and from an APD Homeland camera. (*Id.* at 10-11). According to the Government’s description in the warrant application, the surveillance footage shows five vehicles turning right off of McDaniel Street onto Delevan Street SW and parking outside the grocery store on Delevan Street at approximately 9:40 p.m., and multiple people getting out of multiple vehicles. (*Id.* at 11). The location where Demetrius Davis was shot and killed did not appear in camera view. (*Id.*). However, according to the Government, one of the cameras captured a person exiting a sedan, taking a rifle out of the trunk of the vehicle, and then running outside the camera frame, likely toward Mr. Davis, who was also outside the camera frame. (*Id.*). The Government maintains that the same person with the weapon then backs up into the frame again while shooting the rifle multiple times. (*Id.*). The footage then shows the vehicles driving away from the scene at approximately 9:44 p.m. (*Id.*).

The FBI did not investigate the murder of Demetrius Davis until after the arrests of the 30 NTG members and associates named in the First Superseding

³ The Court’s factual description of Demetrius Davis’s murder in this Order is taken from the Government’s first search warrant application at issue in the instant motion, as indicated by the citations to that warrant. By reciting the factual description from the first search warrant application, the Court does not thereby adopt any of these facts as findings of the Court.

Indictment on October 12, 2017. (*Id.* at 11 n.1). Following the arrests, a cooperating witness who was present at the scene of the murder provided information to law enforcement implicating Defendant. (*Id.* at 10-12). Specifically, the cooperating witness reported that, after an NTG member known as “Bookmen” was killed in the early morning hours of November 22, 2014, Mr. Brown told a group of fellow NTG members at a candlelight vigil later that night that “everyone was going to put in work for Bookmen,”⁴ and he sent multiple crews of NTG members throughout the Atlanta area to hunt for and retaliate against rival Crips gang members based on rumors that the Crips had murdered Bookmen. (*Id.* at 10). The cooperating witness identified approximately 15 people who were in the various vehicles at the scene of Demetrius Davis’s murder and specifically pinpointed Mr. Brown as the shooter. (*Id.* at 12).

A. First Search Warrant

Five years after the shooting incident at issue, and based on the information from the cooperating witness, FBI Special Agent Jason Cleary applied for the first geofence warrant described above, asserting there was “probable cause to search information in the possession of Google relating to what devices were in the Target Location.” (*Id.* at 12). The “Target Location” was a roughly 20-by-50-meter area⁵

⁴ The Government contends that the term “put in work” is NTG slang for criminal activity, including acts of violence. (First Warrant, Doc. 1709-1 at 10; *see also* Second Superseding Indictment, Doc. 1158 at 9.)

⁵ Specifically, the First Warrant sought location history data from all users within a rectangular geographical area defined by the following four latitude/longitude coordinates connected by straight lines:

covering the area where Davis's body was found and where the five vehicles were parked on November 22, 2014. (*Id.*). Agent Cleary further limited the requested search to the time period of 9:35 to 9:56 p.m., "based around the timestamp on the APD Homeland surveillance camera, as well as information that identifies the Google accounts with which those devices are associated, for evidence of the crime(s) at issue in this case." (*Id.*).

Relevant to certain of Defendant's arguments in the Motion to Suppress, Agent Cleary stated in the first search warrant dated September 26, 2019 that he anticipated Google would disclose the information to the government in three stages:

- a. Google will be required to disclose to the government an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported their location within the Target Location described in Attachment A during the time period described in Attachment A.
- b. The government will then review this list in order to prioritize the devices about which it wishes to obtain associated information.
- c. Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires.

(*Id.* at 13).

-
- Point 1: 33.726930, -84.401636
 - Point 2: 33.726763, -84.401643 (approximately 20 meters south of Point 1)
 - Point 3: 33.726748, -84.402187 (approximately 50 meters west of Point 2)
 - Point 4: 33.726932, -84.402199 (approximately 20 meters north of Point 3 and 50 meters west of Point 1)

Magistrate Judge Justin Anand signed the First Warrant. In response to the First Warrant, Google provided the FBI with anonymized information relating to four devices with location history data showing they were within the geofence, consistent with the first step of the warrant. [Doc. 1709 at 14.] Agent Cleary then asked Google to provide the device identification and user information for the four devices. (Third Search Warrant Application (“Third Warrant”), Doc. 1709-3 at 12 (“On November 14, 2019, Google provided the initial anonymized results [in response to the First Warrant], which consisted of four accounts. Your affiant requested that Google provide the device identification and subsequent user information.”)). Among the returns from Google was a WiFi connection within the geofence at 9:52:50 p.m. from an account with the email address pistolplay31@gmail.com and recovery email address terrybrownjr5@yahoo.com. (Second Search Warrant Application (“Second Warrant”), Doc. 1709-2 at 12). The return also included the phone number and Google Account ID number associated with the account.

B. Second Search Warrant

On January 29, 2020, Agent Cleary submitted a second search warrant application to Magistrate Judge Catherine M. Salinas, requesting information associated with Terry Brown’s email account (pistolplay31@gmail.com) and Google Account ID number, as identified in the First Warrant. (Doc. 1709-2). In support of the Second Warrant, Agent Cleary detailed information obtained from the cooperating witness and a wiretap implicating Mr. Brown in various crimes,

including the Demetrius Davis murder. (*Id.* at 6-14). Agent Cleary also explained that the First Warrant had returned information indicating that a device associated with Mr. Brown's email address and Google Account ID number was present within the geofence encompassing the location and time of the Davis murder. (*Id.* at 12). Based on that information, Agent Cleary sought to obtain information (including location history data) from Google related to that email account and Google Account ID number during specific dates and times corresponding with the crimes, including as relevant here the dates of November 22, 2014 at noon to November 25, 2014 at noon. (*Id.* at 14, 28-32). Judge Salinas signed the Second Warrant the same day. (*Id.* at 33).

C. Third Search Warrant

On February 28, 2020, Agent Cleary submitted a third search warrant application to this Court, this time to Magistrate Judge Christopher C. Bly. (Third Warrant, Doc. 1709-3). The Third Warrant, like the First Warrant, sought information related solely to the Demetrius Davis murder. (*Id.*). According to Agent Cleary's supporting affidavit, on February 14, 2020, Google provided the return for the Second Warrant, which contained three additional location data points placing Mr. Brown's device near the site of the Davis murder between 9:53 and 9:56 p.m. that night. (*Id.* at 13). Although these three additional locations were near the Davis murder, they were outside the geographical area specified in the First Warrant. (*Id.*). Agent Cleary thus concluded that the area defining the geofence in the First Warrant was too small, and that requesting a geofence for a

larger area may provide more information about other people involved in the crime. (*Id.*). Accordingly, he requested the location history data and identifying account information of Google subscribers within a larger octagonal geofence, with an area of approximately 24,230 square meters,⁶ during the time frame between 9:50 p.m. and 9:56 p.m. on November 22, 2014. (*Id.* at 16-17). Judge Bly signed the Third Warrant the same day. (*Id.* at 20).

D. Motion and R&R

Mr. Brown moves to suppress all evidence obtained from the three warrants on several grounds. Specifically, he contends that the first geofence warrant was an impermissible general warrant, that it lacked particularity and probable cause, and that the government did not obtain proper judicial approval before obtaining Mr. Brown's Google location history data. Additionally, he contends that the

⁶ Specifically, the Third Warrant sought location history data for an octagon with the following eight latitude/longitude coordinates, connected by straight lines:

- Point 1: 33.727876, -84.401632
- Point 2: 33.727425, -84.402562
- Point 3: 33.726906, -84.402769
- Point 4: 33.726431, -84.402584
- Point 5: 33.726049, -84.401830
- Point 6: 33.726361, -84.401066
- Point 7: 33.726895, -84.400814
- Point 8: 33.727479, -84.401117

(Doc. 1709-3 at 16). These coordinates reflect a distance of approximately 200 meters between the top and bottom of the octagon and approximately 180 meters between the westernmost and easternmost points, as well as a total distance of approximately 570 meters (or 1/3 of a mile) if one were to walk a straight line through each point beginning and ending at Point 1. The address of the grocery store next to the site of the Davis Murder, 1029 McDaniel Street SW, is roughly in the center of the octagon.

subsequent two warrants arising from the first should be treated as fruit of the poisonous tree. [Doc. 1709].

The Magistrate Judge issued a thoughtful and instructive R&R on the Motion to Suppress on September 19, 2023, providing an exhaustive overview of the state of the existing jurisprudence on geofence warrants at that time and ultimately recommending that the motion be denied. [Doc. 1755]. As stated above, Defendant has filed objections to the R&R, [Doc. 1760], and the Government filed a response to the objections (Doc. 1764). In addition to the objections briefing, upon the Court's order, both parties submitted supplemental briefing on the circuit court decisions in *United States v. Davis*, 109 F.4th 1320 (11th Cir. 2024), *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), and *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2024). All three opinions deal with the issue of geofence warrants but post-date the Magistrate Judge's R&R on the instant motion.⁷ [See Doc. 1755 at 4 (the Magistrate Judge noting in the 2023 R&R that "no federal appeals court [] has yet ruled on this emerging area of the law, though two of the district court geofence cases [*Smith* and *Chatrie*] are currently on appeal before the Fourth and Fifth Circuits.")].

The Court has reviewed all of the supplemental authority briefed by the parties in addition to the cases discussed in the R&R to aid in its consideration of

⁷ After the parties submitted their supplemental briefing on these circuit court opinions in October 2024, the Fourth Circuit granted a rehearing en banc in *Chatrie* and issued a 126-page decision comprising eight concurring opinions and one dissenting opinion on April 30, 2025. *United States v. Chatrie*, 136 F.4th 100 (4th Cir. 2025) (en banc).

the unsettled and controversial Fourth Amendment question of the validity of geofence warrants. After careful review, the Court concludes that, although the first geofence warrant was lacking in sufficient particularity at step two, which impermissibly allowed law enforcement unfettered discretion to obtain the identity of any person whose location history data placed him or her near the scene of a crime without any additional probable cause, exclusion is not warranted in this case under the good-faith exception.

II. Standard of Review

A district judge has broad discretion to accept, reject, or modify a magistrate judge's proposed findings and recommendations. *United States v. Raddatz*, 447 U.S. 667, 680 (1980). Pursuant to 28 U.S.C. § 636(b)(1), the Court reviews any portion of the Report and Recommendation that is the subject of a proper objection on a *de novo* basis and any non-objected portion under a "clearly erroneous" standard. "Parties filing objections to a magistrate's report and recommendation must specifically identify those findings objected to. Frivolous, conclusive or general objections need not be considered by the district court." *Marsden v. Moore*, 847 F.2d 1536, 1548 (11th Cir. 1988).

III. Legal Standard

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. Historically, the Fourth Amendment search doctrine was "tied to common-law trespass, at least until the latter half of the 20th

century[,]" because the Fourth Amendment "was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 565 U.S. 400, 405 , 406 (2012). Therefore, the focus of older Fourth Amendment jurisprudence was whether the Government "obtain[ed] information by physically intruding on a constitutionally protected area." *Id.* at 406 n.3. But as people began to assert privacy interests in intangible things such as phone conversations or GPS tracking data of their physical movements, the Supreme Court in the latter half of the 20th century "deviated from that exclusively property-based approach," embracing the principle that "the Fourth Amendment protects people, not places[.]" *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). Thus, under the modern interpretation of the Fourth Amendment, "[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, [] official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter v. United States*, 585 U.S. 296, 304 (2018) (internal quotations and citation omitted). *See also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (referring to the modern rule as the "*Katz* test").

Although this modern formulation of Fourth Amendment standing derived from *Katz* reflects an "expanded" conception of privacy rights under the Amendment, the Supreme Court has explained that the analysis is nonetheless "informed by historical understandings 'of what was deemed an unreasonable

search when the Fourth Amendment was adopted.” *Id.* at 304-05 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)) (internal alterations omitted). The *Carpenter* Court specifically outlined two “basic guideposts” encompassing those historical understandings: “First, that the Amendment seeks to secure ‘the privacies of life’ against ‘arbitrary power.’ Second, and relatedly, that a central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’” 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886) and *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

This threshold question of “whether an individual has a reasonable expectation of privacy in the object of the challenged search,” such that a warrant is required relates to the issue of the individual’s Fourth Amendment “standing.” *United States v. Ross*, 964 F.3d 1034, 1040 (11th Cir. 2020). However, where, as here, the challenged search **was** conducted pursuant to a warrant, courts often skip this threshold question and focus on whether the warrant is supported by probable cause and sufficient particularity. [See Doc. 1755 at 5-6 (collecting cases where courts skip the standing issue to consider the sufficiency of the warrant).] If so, there is no need to evaluate whether a warrant was required in the first place.

Further, even where probable cause or particularity is found lacking, the Court may nonetheless deny a motion to suppress the fruits of the warrant under the good-faith exception established in *United States v. Leon*, 468 U.S. 897 (1984). *Leon* “stands for the principle that courts generally should not render inadmissible evidence obtained by police officers acting in reasonable reliance upon a search

warrant that is ultimately found to be unsupported by probable cause.” *United States v. Martin*, 297 F.3d 1308, 1313 (11th Cir. 2002). Therefore, the *Leon* good-faith exception dictates that courts should decline to apply the harsh remedy of exclusion to evidence obtained from a constitutionally infirm warrant in all but four limited sets of circumstances. These circumstances include: (1) where the magistrate judge, in issuing the warrant, was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth; (2) where the issuing magistrate judge wholly abandoned his judicial role; (3) where the affidavit supporting a warrant application is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or (4) where a warrant is so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid. *Leon*, 468 U.S. at 923.

IV. Discussion

To give important context to the precise issues at hand, the Court will partially recount the helpful history of the use of geofence warrants provided by the Fifth Circuit in *United States v. Smith*:

Google received its first geofence warrant request in 2016. Since then, requests for geofence warrants have skyrocketed in number. . . . By 2021, geofence warrants comprised more than 25% of all warrant requests Google received in the United States.

. . .

Unlike a warrant authorizing surveillance of a known suspect, geofencing is a technique law enforcement has increasingly utilized when the crime location is known but the identities of suspects are not. Thus, geofence warrants effectively work in reverse from traditional search warrants. In requesting a geofence warrant, law 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.

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.” Google collects data from accounts of users who opt in to Google’s Location History service. Location History is disabled by default. For Location History to collect data, a user must make sure that the device-location setting is activated, and that Location Reporting is enabled. . . . 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 tracking the user’s location across every *app* and every *device* associated with the user’s account. In other words, once a user opts into Location History, Google is always collecting data and storing *all* of that data in the Sensorvault.

...

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.” Thus, Google developed an internal procedure on how to respond to geofence warrants. 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.

...

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.

...

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, if 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. 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. As a general matter, Google imposes no geographical limits on this Step 2 data. 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.

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. 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.

110 F.4th at 821–25 (internal citations, quotations, and alterations omitted).

As should be apparent from the background discussion of the warrants at issue, the three-step process described in *Smith* as the typical geofence warrant process was not followed in this case. However, the Court has included the description of the typical process both to help set the stage for the broader discussion of the constitutionality of geofence warrants in general, and because the Government's deviation from that process partly forms the basis of Defendant's Motion to Suppress. [See Doc. 1709 at 48-52]. Having given that context, the Court will now outline the Magistrate Judge's conclusions in the R&R before turning to Defendant's objections.

A. Report and Recommendation

First, the Magistrate Judge addressed the issue of Fourth Amendment standing and found that the first step of the First Warrant—obtaining an anonymized list of all Google users whose location history data placed them within the geofence surrounding the Davis murder—“does not seem to implicate the Fourth Amendment because it is doubtful a person has a reasonable expectation of privacy over information that cannot be connected to him.” [Doc. 1755 at 27-28]. *Accord Chatrue*, 136 F.4th at 144 (Berner, J., concurring) (“Individuals lack a reasonable expectation of privacy in Location History data that is truly anonymous, meaning that—as evaluated at the time of the government's request, the data is not likely to be traceable to specific individuals. An individual does not have a reasonable expectation of privacy in the mere fact that a certain number of

unknown individuals were located near a public place at a particular time, even if he happened to be one of those individuals.”).

Of course, the location history data provided in response to step one did not stay anonymous for long. At the second step of the First Warrant, the Government was able to learn the identities of all four cell phone users whose location history placed them within the geofence at the time of the murder, by asking Google for the subscriber information for all devices identified at step one. But the Magistrate Judge pointed out that that deanonymized data (i.e., the names and email addresses of the subscribers associated with the devices) is “composed of information that the government can request via administrative subpoena under 18 U.S.C. § 2703(c).” [*Id.* at 28]. Acknowledging that the combination of the two steps—allowing law enforcement to link a person’s Google account to a specific location at a specific time—“may offend notions of privacy[,]” the Magistrate Judge nonetheless concluded that flattening the two steps into one “does not seem to present the kind of privacy concerns that the Supreme Court has guarded against.” [*Id.*]

Specifically, the Magistrate Judge had previously outlined the history of the development of Fourth Amendment standing through various Supreme Court cases. These cases include *Katz*, 389 U.S. at 351 (where, as discussed above, the Court first established the notion that the Fourth Amendment protects “people, not places” and extended its protection to a private conversation in a public phone booth); *Jones*, 565 U.S. at 415-16, 426 (where five Justices concurred that even if

there were no physical trespass required to achieve it, long-term GPS tracking raises Fourth Amendment privacy concerns); *Riley v. California*, 573 U.S. 373, 395-96 (2014) (where the Supreme Court held that a warrant is required to search a person’s cell phone due to the vast quantity of private information they hold, including “[h]istoric location information” that “can reconstruct someone’s specific movements”); and *Carpenter*, 585 U.S. at 309-10 (where the Supreme Court held that a person maintains a reasonable expectation of privacy in cell phone location records notwithstanding the third-party doctrine, due to the “detailed, encyclopedic, and effortlessly compiled” nature of such data). Referring back to this relevant case law, the Magistrate Judge explained that, here, there was no physical trespass beyond public spaces as in *Jones*, no surveillance of a private conversation as in *Katz*, and the information obtained here was essentially a “snapshot” of location history 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 thus distinguished it from the “comprehensive chronicle” of a user’s movements at issue in *Riley* and *Carpenter*. [Doc. 1755 at 28-29]. Thus, he compared the location history data obtained from the First Warrant to 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.” [Id. at 29]. However, the Magistrate Judge clarified that he is “not prepared to conclude that the acquisition of [location history] information never implicates the

Fourth Amendment[,]” – but instead only that a geofence warrant as tightly limited in space and time as the one at issue here likely does not. [*Id.* at 30].

The Magistrate Judge’s analysis did not stop at standing. Instead, since there were indeed three separate search warrants authorizing the FBI to obtain the location history data at issue, the Magistrate Judge went on to address whether the warrants were supported by probable cause and particularity, ultimately concluding that they were. [*Id.* at 21-40]. Lastly, the Magistrate Judge found that even assuming the warrants were not supported by sufficiently particularized probable cause, suppression is not the appropriate remedy because the *Leon* good-faith exception would apply. [*Id.* at 40-41].⁸

B. Objections

Defendant objects to the R&R in its entirety and requests a *de novo* review of the Motion to Suppress. [Doc. 1760]. First, Defendant contends he has a protected Fourth Amendment interest in his location history data, not only because he has a reasonable expectation of privacy in the data, but also because he has a property interest in the data. [*Id.* at 17-26; 30-33]. Defendant also presents argument in response to the Government’s contention in the initial briefing that the Court should apply the third-party doctrine to find Mr. Brown lacks a

⁸ The Magistrate Judge also recommended that Defendant’s Preliminary Motion to Suppress Evidence [Doc. 1707] be denied as moot in light of the Government’s withdrawal of its opposition to that motion. [Doc. 1755 at 2 n.1; *see also* Doc. 1754 (Government’s withdrawal of its opposition and representation that it will not use the evidence at issue in its case-in-chief).] The Court will adopt this recommendation and **DENY** Defendant’s Preliminary Motion to Suppress [Doc. 1707] **as moot**.

reasonable expectation of privacy in information he voluntarily conveyed to Google. [*See id.* at 26-30; Doc. 1730 at 10-14].⁹ Next, Defendant asserts that the warrants at issue lacked probable cause, particularity, and appropriate judicial approval. [*Id.* at 33-49]. He also rejects the Magistrate Judge's finding that the good-faith exception would apply to foreclose suppression as a remedy here. Defendant asserts the good-faith exception is inapplicable because the deficiencies of the First Warrant were so readily apparent that no reasonable law enforcement officer could have presumed it would be valid, and that the FBI willfully skipped the second step of the First Warrant by asking for subscriber information for all accounts identified at step one rather than prioritizing some accounts over others. [*Id.* at 50-51].

Defendant further requests an evidentiary hearing to address how the two-step process outlined in the First Warrant skipped a step typically present in geofence warrants (i.e., step two of the three-step process outlined above), and the nature and ramifications of the process that law enforcement and Google followed in this case instead. [*Id.* at 8-9]. The Court finds an evidentiary hearing is unnecessary, because Defendant adequately explains his arguments on every point on which he requests a hearing in the papers. In light of the objections, the Court will conduct a *de novo* review of the Motion to Suppress, first addressing the issue of Fourth Amendment standing and the related third-party doctrine, and then

⁹ Although Defendant makes this argument in his objections to the R&R, the Court notes that the applicability of the third-party doctrine is not in fact discussed in the R&R.

considering Defendant's arguments regarding the sufficiency of the warrants and the applicability of the good-faith exception.

C. Fourth Amendment Standing and the Applicability of the Third-Party Doctrine

Whether Defendant has Fourth Amendment standing—that is, a reasonable expectation of privacy in his location history data—necessarily dovetails with the question of whether the third-party doctrine should apply to find that people lose any such reasonable expectation in information they willingly share with third parties. Therefore, the Court addresses the two issues together.

As discussed in the R&R, the jurisprudence governing individuals' reasonable expectation of privacy with respect to personal information that could be gleaned from their cell phones has diverged from earlier related caselaw. Prior precedent primarily focused on whether the conduct of the person whose privacy was at stake and who objected to the search had taken sufficient steps to maintain privacy and protect the information or items at issue from all other eyes. *See, e.g., United States v. Miller*, 426 U.S. 435, 440-46 (1976) (holding that an individual has no reasonable expectation of privacy in his bank records, which were seized by the Government via subpoena without a warrant, on the basis that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed”); *Smith v. Maryland*, 442

U.S. 735, 739-46 (1979) (applying the same rationale that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties” to find, in a case involving a challenge to a pen register, that an individual holds no reasonable expectation of privacy in records of phone numbers he dialed). *Miller* and *Smith* represent the origin of the so-called “third-party doctrine,” which eliminated for a time the idea that a person could have a reasonable expectation of privacy in anything he had willingly shared with a third party.

After the Supreme Court’s decisions in *Riley* and *Carpenter*, however, there has been a shift in focus from the conduct of the person who wants to keep something private to the nature of the thing itself. The Supreme Court in both cases took pains to emphasize how comprehensive and intimate the information stored on a cell phone can be, and how frightening a prospect it is that law enforcement might use a world of ever-increasing documentation to its advantage by requesting dossiers of retrospective, comprehensive, minute-by-minute records of any citizen’s every movement, at little to no cost to the Government. It is difficult to square these opinions with older cases that inquired instead into whether the conduct of the defendant evinced a sufficiently secretive attitude toward his own affairs. Thus, although the *Carpenter* court made clear that it was not overturning the third-party doctrine altogether, it at least changed the calculus when it comes to location data tracked through a person’s cell phone.

Specifically, in *Carpenter*, the Supreme Court rejected the Government’s argument that the third-party doctrine should apply to cell-site location

information (“CSLI”), which—similar to location history—is information that can be used to create a record of a person’s movements from data collected automatically by cell phone towers when users make or receive phone calls. In refusing to apply the third-party doctrine, the Court explained:

The Government’s position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

Carpenter, 585 U.S. at 313-14.

The *Carpenter* court didn’t stop there—it also emphasized that even where a person “knowingly share[s]” information with a third party, the Fourth Amendment does not “fall[] out of the picture entirely” such that the person loses **any** expectation of privacy in the information. *Id.* at 314 (quoting *Riley v. California*, 573 U.S. 373, 392 (2014)). Rather, his expectation of privacy is merely reduced, and courts are called upon to consider not only whether the information at issue was knowingly shared, but also “the nature of the particular documents sought” to determine whether “there is a legitimate expectation of privacy concerning their contents.” *Carpenter*, 585 U.S. at 314 (quoting *United States v.*

Miller, 425 U.S. 435, 442 (1976)). If so, the information remains entitled to Fourth Amendment protection.

Perhaps most importantly of all, the *Carpenter* court emphasized that the Supreme Court has shown “special solicitude for location information in the third-party context” and repeatedly tethered its decision to the fact—said many times and in many different ways—that CSLI creates “a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.” 585 U.S. at 315. *See also id.* at 300, 309, 311, 312, 315 (referring to CSLI throughout the opinion as “a comprehensive chronicle of the user’s past movements”; “an all-encompassing record of the holder’s whereabouts”; “near perfect surveillance,” akin to attaching “an ankle monitor to the phone’s user”; “a detailed and comprehensive record of the person’s movements”; a “comprehensive dossier of [a person’s] physical movements”).

The Supreme Court’s decision in *Carpenter* represented a “sea change” in how the Supreme Court specifically treats location tracking data transmitted from a person’s cell phone—as distinguished from other forms of intangible information such as bank or telephone records or even surveillance footage documenting a person’s movements in a public area. *Chatrie*, 136 F.4th at 119 (Wynn, J., concurring) (quoting Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1799–1800 (2022)). That is, the *Carpenter* Court pulled back from the granular in-the-weeds analysis of how such data is transmitted to and stored by third parties, to instead

focus on the broader principles animating the Fourth Amendment. Recognizing cell-site records as a “qualitatively different category” of information from the telephone numbers and bank records at issue in *Smith* and *Miller*, the *Carpenter* court explained: “After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, **but a detailed and comprehensive record of the person’s movements.**” 585 U.S. at 309 (emphasis added). Thus, due to the character of the information at issue—its comprehensiveness and the fact that it tracks a person’s physical movements—the Court expressly declined to extend the third-party doctrine from *Smith* and *Miller* “to cover these novel circumstances” and held “that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Id.* at 309-10. “In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.” *Carpenter*, 585 U.S. at 320.

But again, while this ruling may have dealt with a novel type of information and changed how the third-party doctrine is applied, it remained tethered to the original aims of the Fourth Amendment— “to secure the privacies of life against arbitrary power” and “to place obstacles in the way of a too permeating police surveillance.” *Carpenter*, 585 U.S. at 305. Put another way by Judge Wynn in his excellent concurrence in *Chatrie*, “[i]nstead of ‘mechanically applying the third-

party doctrine,’ *Carpenter* applied a new framework rooted in historical understandings of Fourth Amendment privacy rights but adapted to the particular surveillance technology at issue.” *Chatrie*, 136 F.4th at 120 (Wynn, J., concurring) (quoting *Carpenter*, 585 U.S. at 314).

We live in an age when many of the most vital and intimate parts of what we might deem integral to our private selves or our activities have been embedded in the cloud. Often, they are stored there intentionally to allow us later to save and revisit cherished memories, or perhaps for the more mundane administrative purposes of quickly locating tax returns or insurance information when needed on the fly. But much of this information storage is automatic, unthinking, just another feature of one of the dozens of apps we have on our phones. Ours is an era of convenience, where the near-constant documentation of our lives murmurs along steadily in the background of our living. We are accustomed to it and often give no thought to it. A maps or rideshare app prompts us to turn on location services to improve location accuracy, and we agree. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 936 (E.D. Va. 2022), *aff’d on reh’g en banc*, 136 F.4th 100 (4th Cir. 2025) (“While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, 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.”). It proves more challenging with each passing year to apply 18th-century or even 1970s-era understandings of privacy to

a world where faceless, voiceless, corporate or government “third parties” collect deeply sensitive information through automatic processes on our phones or other smart devices as we go about our days. It is for these reasons that “the third-party doctrine is an increasingly tenuous barometer for reasonable privacy expectations in the digital era.” *Chatrie*, 136 F.4th at 119 (Wynn, J., concurring).

As described above and in the Supreme Court’s *Carpenter* opinion, the modern rule from *Katz* is that “[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.” *Carpenter*, 585 U.S. at 304. So written, the rule appears simple and straightforward in its application. But courts have struggled mightily to apply it faithfully in the five decades since *Katz*. For example, it is difficult to reconcile this formulation of the rule with the holding in *Miller* that bank records can be obtained without a warrant. Certainly, society generally recognizes bank records as private—so private they are password-protected and often doubly hidden behind two-factor authentication to boot. Yet longstanding precedent in the form of the third-party doctrine dictates that, because we allow bank employees access to such information, we would be *unreasonable* to expect that law enforcement be denied the same ready access. That did not ring true to many reasonable minds in the 1970s when *Miller* was decided and, since that time, the doctrine has become even more “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). *See also, e.g., Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (“Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”).

Of course, it is not this Court’s task to “reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). But the Court points to these ongoing debates among judges in the Courts of Appeals and justices on the Supreme Court to illustrate how an elegant rule statement has proven not-so-elegant in its real-world application in a rapidly changing technological landscape. The Fourth Circuit’s recent *en banc* decision in *Chatrle* is illustrative. Across eight concurrences and one dissent, perhaps every conceivable stance on this thorny question was taken. After careful, considered review, this Court finds the most persuasive of the opinions to be Judge Wynn’s concurrence. In that opinion, Judge Wynn outlined the four features of cell site location data that the *Carpenter* Court identified to set it apart as “qualitatively different” from other forms of information: its comprehensiveness, the capacity for retrospective tracking, the intimacy of the information revealed, and the ease of access for police. *Chatrle*, 136 F.4th at 120; *Carpenter*, 585 U.S. at 309-13. The Court agrees that these four factors apply with equal or greater force to the location history data at

issue in this case, requiring a finding that Defendant had a reasonable expectation of privacy in that data. Considering the vast amount of location history data stored by Google, geofence warrants threaten just such a “permeating police surveillance” if location history data is left unshielded by Fourth Amendment protection on the basis of the third-party doctrine.

Moreover, the Court is not persuaded by the Magistrate Judge’s finding that the temporal and geographic constraints on the geofence warrant in this case sufficed to remove any Fourth Amendment protection. [See Doc. 1755 at 28-30]. “*Carpenter*’s retrospectivity analysis emphasized the vast scope of *available* CSLI data, which gives police ‘access to a category of information otherwise unknowable.’” *Chatrle*, 136 F.4th at 122 (Wynn, J., concurring) (quoting *Carpenter*, 585 U.S. at 312) (emphasis in *Chatrle*). Judge Wynn rightly noted that the Supreme Court in *Karo* found that “tracking even an *object*’s trip in and out of a private space” is a search, and location history is capable of tracking *people* in and out of private spaces “with even greater precision than CSLI or the beeper in *Karo*.” *Chatrle*, 136 F.4th at 124. Moreover, “[i]n light of the intimately revealing nature of Location History data, the span of time it covers is of little importance to the Fourth Amendment search analysis.” *Id.* The Court agrees and finds that an individual does have a reasonable expectation of privacy in his location history data, no matter how limited the geofence is to a particular time and place.

Here, of course, Mr. Brown’s location history data ***was*** obtained pursuant to a search warrant after a showing of particularized probable cause was found to

have been made. Turning then, to Mr. Brown's second argument in support of the motion to suppress, the Court will evaluate whether the warrant applications were supported by probable cause and sufficient particularity.

D. Probable Cause and Particularity

In determining whether probable cause exists in support of a search warrant, "[t]he task of the issuing magistrate 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 of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The Court "usually requires 'some quantum of individualized suspicion' before a search or seizure may take place." *Carpenter*, 585 U.S. at 317 (quoting *United States v. Martinez-Fuerte*, 428 U.S. 543, 560-61 (1976)).

Defendant challenges all three warrants in this case as impermissible "general warrants." [Doc. 1709 at 17-27]. A general warrant is one that "specifie[s] only an offense" and leaves it to the discretion of the executing officials to make "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). The Supreme Court has explained that the Framers crafted the Fourth Amendment as a "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. Defendant's argument on this point is consistent with the Fifth Circuit's holding in *Smith*, where the court

concluded that that geofence warrants present the exact sort of “general, exploratory rummaging” that the Fourth Amendment was designed to prevent. *Smith*, 110 F.4th at 837 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). Specifically, because Google does not store location history data in a way that enables it to search a specific area, “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.” *Smith*, 110 F.4th at 824. The Fifth Circuit treated that initial search of the Sensorvault done by Google as the relevant “search” by law enforcement for Fourth Amendment purposes, which directly informed its holding. *See Smith*, 110 F.4th at 837-38 (“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.”). Following that premise, the Fifth Circuit concluded that “geofence warrants are general warrants categorically prohibited by the Fourth Amendment.” *Id.* at 838.

To be clear, the Court joins in the Fifth Circuit’s alarm at the Government’s widespread use of geofence warrants to drum up suspects out of thin air in the absence of other evidence. It runs counter to deeply rooted Fourth Amendment principles to permit the Government to ask Google to conduct a retrospective search of the location history data of hundreds of millions of users and to return to the Government a list of all persons within the vicinity of a crime. However, the

facts of the case at issue here do not support this Court's holding that the warrants were impermissible general warrants.

In the First Warrant, Agent Cleary laid out in detail the information the FBI had obtained from a cooperating witness implicating Mr. Brown and others in the Davis murder. (Doc. 1709-1 at 10-12). Based on that information, the Court finds that Agent Cleary had probable cause to seek out corroborating evidence regarding whether the NTG members identified by the cooperating witness were indeed present at the scene of the Davis murder. The Court also agrees with the Magistrate Judge's reasoning in the R&R that the geofence in the First Warrant was tightly confined to the area of the murder and to a narrow timeframe when the murder occurred. The Court departs from the Fifth Circuit's rationale here, because the Government did not conduct a "search" of the whole of Google's database of location history information. Rather, Attachment A of the First Warrant permitted the Government to search only the location history data of devices "that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below"—that is, the 20-by-50-meter area surrounding the scene of the Davis murder during the time period of 9:35 p.m. to 9:56 p.m. on November 22, 2014. (Doc. 1709-1 at 15). From there, the Court authorized Google to "query location history data based on the Initial Search Parameters specified in Attachment A" and to "produce to the government anonymized information specifying the corresponding unique device ID, timestamp. Coordinates, display radius, and data source, if available[.]" (*Id.* at 16).

Even if Google’s internal processes require that it start with all user information within its database before producing the information specified in the warrant, it does not follow that the Government conducted a search of the whole of the database. The Government was not authorized to search or seize any location history information for any devices outside of the geofence, nor did it do so. For that reason, the first step of the First Warrant—allowing Agent Cleary to obtain an anonymized list of devices within the geofence at the time of the Davis murder—was supported by probable cause to believe that Google’s return from its database would help inculcate or exculpate the NTG members identified by the cooperating witness as having been involved in the Davis murder. The Court thus rejects Defendants’ argument that this step constituted the sort of impermissible “general, exploratory rummaging” that the Fourth Amendment was designed to prevent. The warrants at issue here laid out sufficient probable cause to suspect Mr. Brown of specific criminal racketeering activity, and Agent Cleary gave reasons why the location history data sought might provide further evidence of those crimes.

Defendant’s next argument, however, fares better. Defendant contends that step two of the First Warrant gave the Government “unbridled discretion to obtain identifying information . . . for all devices identified in step one” without any basis to prioritize specific devices. [Doc. 1709 at 5]. Noting that Agent Cleary did not follow the standard geofence warrant three-step process in this case,¹⁰ Defendant

¹⁰ As discussed *supra* at 6, the three-step process authorized by the First Warrant is as follows: at Step One, Google was required to disclose to the government an anonymized list of devices that specified information including the corresponding unique device ID, timestamp, coordinates, and

argues that the agent's failure to request a second anonymized list of location history data for a smaller subset of subscribers identified as being within the geofence in response to the First Warrant should lead the Court to conclude that there was no probable cause to obtain identifying information for any anonymous device identified at step one (including Mr. Brown's), as requested at step two. [*Id.* at 4-6].

Even if there is sufficient probable cause to search location history data that might reveal evidence of who was involved in a crime, a search warrant may nonetheless be found invalid for lack of particularity. For example, a warrant may be found to lack sufficient particularity if it permits law enforcement "unbridled discretion" in how to narrow the list of anonymized users provided at step one before requesting subscriber information for a subset of those users, without any criteria specified in the warrant for how the list will be culled. *See, e.g., Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 88 (D.D.C. 2021); *Matter of Search of Info. Stored at Premises Controlled*

data source, if available, of the devices that reported their location within the Target Location described in Attachment A during the time period described in Attachment B (i.e., devices within the geofence). At Step Two, the government then reviewed this list in order to prioritize the devices about which it wished to obtain associated information. At Step Three, Google was then required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquired. (First Warrant, Doc. 1709-1 at 13). Google's internal procedures for responding to geofence warrants anticipates that law enforcement will narrow the list of device IDs identified at Steps One and Two before requesting subscriber information for particular devices at Step Three. *See Chatrie*, 136 F.4th at 132-33; *Smith*, 110 F.4th at 824-25. In contrast, here, Agent Cleary requested and received from Google the identifying subscriber information for all four devices that were identified as present within the geofence at Step One. (Doc. 1709-3 at 12).

by Google, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020); *People v. Meza*, 90 Cal. App. 5th 520, 536-38 (Cal. Ct. App. 2023). That was the case here.

Pursuant to the First Warrant, Agent Cleary was given judicial approval to obtain an anonymized list of Google subscribers whose location history data indicated they were within the 20-by-50-meter geofence during a six-minute period around the time of the Davis murder. (Doc. 1709-1, First Warrant at 15-16). From there, according to the First Warrant, the Government stated that it would “review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information” and that Google would then be “required to disclose to the government identifying information [i.e., subscriber names and email addresses] for the Google account associated with each device ID about which the government inquires.” (*Id.* at 16).

However, there was nothing in the First Warrant to limit the Government’s ability to obtain identifying information for **all** devices within the geofence. Simply because there was probable cause to suspect Defendant of being involved in the Davis murder, it does not follow that there was probable cause to believe that **all** devices connected to Google accounts within the immediate vicinity of the murder contained evidence of a crime. Step two of the First Warrant—allowing Agent Cleary to request subscriber information from Google for all devices identified at step one, without any additional probable cause to suspect that each of those devices belonged to someone involved in the crime or otherwise contained evidence of a crime—lacked the “quantum of individualized suspicion” required.

Carpenter, 585 U.S. at 317. That aspect of the First Warrant was therefore lacking in sufficiently describing particularized probable cause. *See Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 88 (D.D.C. 2021) (explaining that a geofence warrant that “proposed no rule or condition that would adequately cabin” the discretion of law enforcement at step two to request identifying information about the anonymized devices identified at step one violated the particularity requirement, and that the typical second step of requiring law enforcement “to return to the Court and justify any device deanonymization based on its review of the anonymized information provided by Google and other evidence in the case . . . ensures that the government’s search is particularized; that is, before any identifying information is disclosed to the government, it must justify the specific devices for which it seeks that information, consistent with its showing of probable cause.”); *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (finding the particularity requirement was not met by a geofence warrant that, like the one at issue here, “puts no limit on the government’s discretion [at step two] to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences” because “[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the

identifying subscriber information, and thus, those persons' location histories.") (internal citation omitted).

On this point, the Court agrees with Defendant that a person's presence at or near a crime scene during a 21-minute period when a crime occurred does not by itself amount to probable cause justifying a search. There is an easy parallel here to the principle that "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. Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). *See also Chatrue*, 136 F.4th at 153 (Berner, J., concurring) ("Before the first request to Google, the detective could make a single representation about the Google users he would ultimately search: they would be among those near the crime scene. That information unequivocally falls short of establishing probable cause. . . . [A] warrant can authorize the search of all persons in a particular place only if there is probable cause to believe every person in that place was involved in or witnessed the criminal activity.").

Of course, the counterpoint to applying that principle to the case at hand is the argument that obtaining location history data is not a search or seizure of the **person** whose movements are logged in minute detail therein, but rather something akin to obtaining surveillance footage or other records from a third party. The Court finds *Carpenter* forecloses that counterpoint, for the reasons already explained in the Court's Fourth Amendment standing analysis. Because of

the sensitive nature of location history data and the comprehensive tracking that could be conducted with unfettered access to that data, a warrant allowing the Government to obtain a person's location history, based solely on a person's proximity to a crime scene, and with no protective cloak of anonymity, violates the Fourth Amendment. Therefore, although the Government had probable cause to obtain Defendant's location history data in particular based on the information from the cooperating witness that he was the shooter, it did not have sufficiently particularized probable cause to obtain the identity of every person who happened to be within the geofence defined in the First Warrant.

The Court acknowledges the point made by the Magistrate Judge that, pursuant to that section of the Stored Communications Act, law enforcement is entitled to obtain subscriber information for any device ID that it so requests. However, the Government should have been required to describe with sufficient particularity the criteria it would apply to "prioritize" certain devices identified in step one before seeking out subscriber information from Google for those devices pursuant to 18 U.S.C. § 2703(c)(2). Because law enforcement would not have been able to identify the device IDs for which subscriber information was needed without the use of the geofence at step one, and because there were no limiting criteria at step two, the First Warrant effectively allowed the Government to obtain the names and email addresses of ***every person*** within the geofence who was carrying a cell phone with location history enabled.

It is worth noting here that there were far more than four people present within the geofence, according to both the testimony of the cooperating witness and the surveillance video footage. This discrepancy is not inexplicable—some of the people within the geofence may not have had Google-connected phone devices on their persons, and others likely did not have the Location History feature enabled. Many people own basic phones that do not have the capability of connecting to Google applications at all, and that may have been all the more true in 2014 when the shooting occurred here. And, even if there were other people beyond the four who had Google-connected devices with Location History enabled, they may not have been captured within the geofence because, “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.” *Smith*, 110 F.4th at 824. “Google represents that for any given location point, there is a 68% chance that a user is somewhere within the confidence interval.” *Chatrie*, 107 F.4th at 323, *vacated on reh’g en banc on other grounds*, 136 F.4th 100 (4th Cir. 2025). In other words, the list of four people that the Government received from Google in response to the First Warrant represented an arbitrary subset of all the people who were actually within the geofence. That arbitrariness raises another concern. In a cold case where the Government is fishing blindly for leads, a list like the one in this case could lead investigators to narrow their focus—without good reason—to the people who happened to be captured within the geofence. The Government’s use of geofence

warrants to build a suspect list in the first instance could thus unfairly stack the deck against those people who happened to be included on Google's incomplete and possibly inaccurate list of people in the vicinity of the crime, by creating a perception on the part of law enforcement that the perpetrator must be within that artificially limited suspect pool. The danger of that kind of arbitrariness is precisely why the Fourth Amendment demands a showing of particularized probable cause to justify a search.

In sum, a person's mere propinquity to a crime scene is not alone probable cause to suspect him of a crime. It follows, then, that the Government should not be permitted to obtain the names and email addresses—that is, the identities—of just any person who is near a crime scene at the time a crime occurred, without some evidence that this person was involved in or witnessed the crime.

This constitutional infirmity could have been resolved had there been judicial oversight at the second step of the warrant requiring the Government to prioritize the devices within the geofence for which subscriber information would be sought based on particularized criteria subject to further judicial approval, such as, for example, the length of time spent within the geofence, the specific locations within the geofence where the devices were located, or whether the path traveled by a given device aligned with the path traveled by the vehicles shown pulling up to the grocery store in the surveillance footage of the murder. Alternatively, the Government could have requested 5-10 additional minutes of the location history data for the four devices identified at step one to determine whether they appeared

to be traveling together before arriving within the geofence before the murder. Any of those approaches would have placed sufficient constraints on the Government's discretion so as to bring the warrant in line with the requirements of the Fourth Amendment.

It may be the case that, even had such criteria been in place, and required by the warrant, the outcome would have been the same with respect to the devices for which the Government was permitted to obtain subscriber information. Indeed, perhaps Agent Cleary had constitutionally sufficient grounds to conclude that there was probable cause to obtain subscriber information for all four devices before he requested it from Google. The Court cannot say from the record before it. But the point here is that the judiciary must closely scrutinize the use of geofence warrants to prevent excessive government intrusion into the intimate communications and activities in our private lives. Pursuant to the provisions in the First Warrant here, Agent Cleary had unfettered authorization to obtain the names and email addresses of all persons who might have been within some relatively close proximity to the Davis murder, whether they were asleep in bed nearby, driving past on the way home, a witness to the crime, or the person pulling the trigger. The only limitation was whether Google had the data to give. That unbridled authority granted to the Government at step two of the First Warrant violated the Fourth Amendment.

E. Good-Faith Exception

Notwithstanding the Court's conclusion that the First Warrant lacked sufficient particularity at its second step, this is a close call. Recognizing that courts disagree extensively on how to apply the Fourth Amendment to the novel question posed by geofence warrants, the Court cannot say that any reasonable jurist or executing officer would have found the warrants at issue in this case to be lacking in sufficient particularity or unsupported by probable cause. For that reason, the Court finds the good-faith exception applies to all three warrants, such that suppression is not an appropriate remedy in this case.

“Exclusion is not a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search.” *Davis v. United States*, 564 U.S. 229, 236 (2011) (quotations omitted). The “sole purpose” of the exclusionary rule is to deter future Fourth Amendment violations. *Id.* Therefore, the exclusionary rule should be used to “deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.” *Herring v. United States*, 555 U.S. 135, 144 (2009). That bar is not met here.

Defendant argues that a reasonable law enforcement officer “could not have presumed that the first geofence warrant, which was an overbroad, unparticularized warrant lacking in probable cause and judicial approval[,] would be valid.” [Doc. 1760 at 50]. This argument echoes the fourth circumstance set forth in *Leon*, justifying exclusion where a warrant is “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the

executing officers cannot reasonably presume it to be valid.” 468 U.S. at 923. The Court disagrees that the warrant is so deficient. Agent Cleary’s affidavits set forth detailed probable cause statements establishing more than sufficient probable cause to suspect Mr. Brown in particular of numerous crimes, and to suspect that he was present at and involved in the murder of Demetrius Davis. The temporal and spatial bounds of the geofence approved in the first warrant were tightly constrained to a small area surrounding the scene of the murder, and the agent explained why he believed the information returned by Google would contain evidence tending to exculpate or inculpate the NTG members implicated by the cooperating witness.

Though the Court finds that step two of the First Warrant was lacking in particularity, as explained above, the warrant was otherwise sound. The warrant could have passed constitutional muster with one additional step baked in to more precisely define how the Government would “prioritize the devices” about which it would seek identifying subscriber information at step two. For example, after Google returned its list of four anonymized devices that were within the geofence, Agent Cleary could have sought additional—but still anonymized—location history data for all four devices immediately before or after the murder. From there, he could have gone back to the Court with probable cause to obtain subscriber information for all four devices if, for example, the additional data showed that all of the devices appeared to move in the same path as the vehicles observed on the surveillance footage, or they all lingered in the area of the murder for the same

amount of time. Under this hypothetical process, there would be particularized criteria allowing the agent to learn the identities of only the people whom he had probable cause to believe were involved in or witnessed the crime.

Moreover, unlike in other geofence warrant cases, Agent Cleary did not apply for the geofence warrant here to generate leads in a completely cold case. Rather, Agent Cleary applied for a geofence warrant only after he had leads from the cooperating witness, who provided information about who was present at the scene of the Demetrius Davis murder and who identified Brown as the shooter. In the probable cause affidavit, Agent Cleary made clear that he was seeking the warrant to corroborate the cooperating witness's story. He did not begin with a blank slate, and he acted in good faith in casting what he believed to be a reasonably limited net—limited in both space and time—to verify the witness account. This evidentiary trail provided probable cause to suspect Mr. Brown of having been involved in this particular shooting and having been at this particular crime scene at the time the shooting occurred, with or without a geofence capturing the location history data of any number of unknown other persons who happened to be within the vicinity, or who were potentially involved in the alleged offense as well.¹¹ For that reason, despite lacking in particularity, the warrant before the

¹¹ Again, as discussed *supra* at 40-41, the cooperating witness informed the FBI that there were approximately 15 total NTG members in the vehicles that pulled up to the grocery store before the shooting, but the first warrant return led to the identification of only four people within the geofence. Agent Cleary stated in the First Warrant application that “[m]ultiple conspirator[s] remain unidentified or validated as present at the murder.” (Doc. 1709-1 at 12). But there is nothing in the record to show what measures, if any, the FBI took to identify other suspects present at the crime scene who did not possess phones

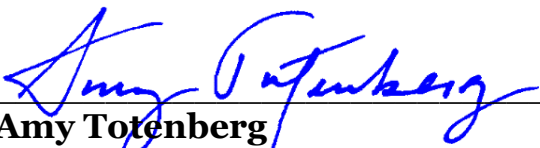
Court does not feel “uncomfortably akin to the ‘reviled’ general warrants that the Framers intended the Fourth Amendment to forbid.” *Chatrie*, 136 F.4th at 122 n.7 (Wynn, J., concurring). Therefore, the Court is not persuaded by Defendant’s argument that the executing officers could not have reasonably and in good faith presumed the warrant to be valid.

V. Conclusion

For the reasons explained above, the Court **ORDERS** as follows:

- (1) Defendant’s Preliminary Motion to Suppress [Doc. 1707] is **DENIED as moot**;
- (2) The Magistrate Judge’s Report and Recommendation [Doc. 1755] is **ADOPTED in part** and **REJECTED in part**;
- (3) Defendant’s Objections to the Report and Recommendation [Doc. 1760] are **SUSTAINED in part** and **OVERRULED in part**; and
- (4) Defendant’s Motion to Suppress Evidence from Warrants and Request for Evidentiary Hearing [Doc. 1709] is **DENIED**.

IT IS SO ORDERED this 13th day of June, 2025.


 Amy Totenberg
 United States District Judge

connected to Google. Such measures, if taken, would mitigate the risk of law enforcement simply zeroing in on the one suspect who had been named by the informant and whom the Government was able to retrospectively track through Google’s location data.